التنظيم القانونى
للبنك الإلكترونى على شبكة الإنترنت



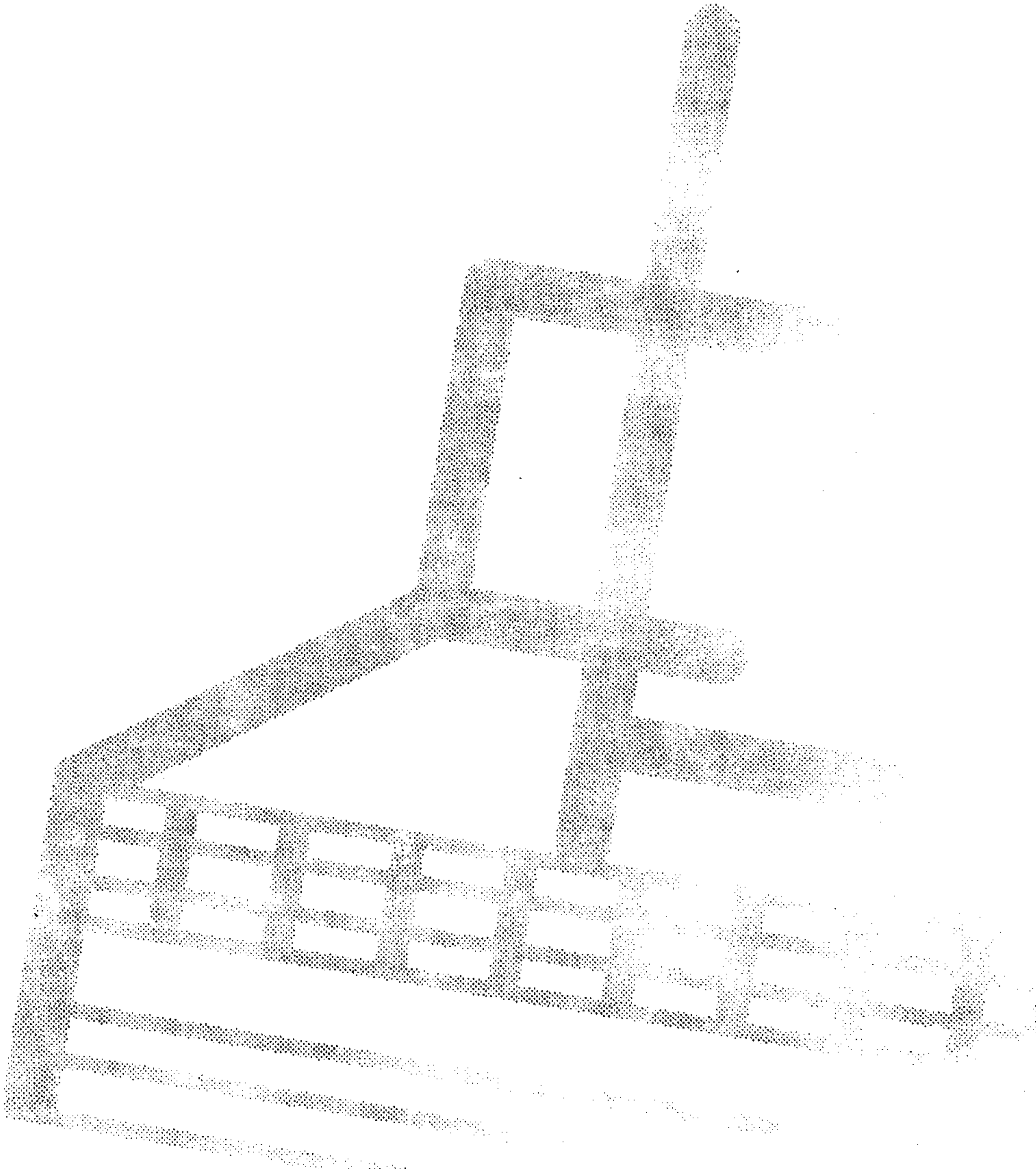
دكتور

علاء التميمى

قسم القانون التجارى

كلية الحقوق - جامعة المنصورة

دار الجامعة الجديدة



دار الجامعة الجديدة للنشر

٣٨ شارع سوتير - الأزاريطة الإسكندرية ت : ٤٨٦٣٦٢٩ - ٤٨٦٨٠٩٩

E-mail. : darelgamaaelgadida@hotmail.com

www.darggalex.com info@darggalex.com

التنظيم القانونى

للبنك الإلكترونى على شبكة الإنترنت

التنظيم القانوني
للبنك الإلكتروني على شبكة الإنترنت

دكتور

علاء التميمي

قسم القانون التجاري

كلية الحقوق – جامعة المنصورة

2012

دار الجامعة الجديدة

٣٨–٤٠ ش سوتير – الأزاريطة – الإسكندرية

تليفون: ٤٨٦٣٦٢٩ فاكس: ٤٨٥١١٤٣ تليفاكس: ٤٨٦٨٠٩٩

E-mail: darelgamaaelgadida@hotmail.com

www.darggalex.com info@darggalex.com

﴿ بسم الله الرحمن الرحيم ﴾

إهــداء

إلى معلم البشرية الأول رسول الله صلى الله عليه وسلم حبًا وإعزازًا.

إلى والدي الغالي، الذي رحل عني قبل أن يرى على غرسه الثمر.

وإلى والدتي التي كانت لي شمعة تحترق كي تضيء لي دربي.

إلى أساتذتي الأجلاء إقرارًا بفضلهم واعترافًا بجميلهم

الباحث

مقدمـــة

١- موضوع البحث:

يتناول هذا البحث بالدراسة اقتراح تنظيم قانوني للبنك الإلكتروني على شبكة الإنترنت في مصر، وذلك في ظل غياب تشريع مصري خاص ينظم إنشاء وعمل هذا البنك. يأتي ذلك في الوقت الذي أضحى فيه هذا البنك واقعا ملموسا يلعب دورا هاما وخطيرا في المعاملات التجارية وغير التجارية.

ويهتم هذا البحث في الأساس بالتنظيم القانوني للعلاقات المستحدثة في نظام عمل البنك على شبكة الإنترنت، التي أفرزتها البيئة الإلكترونية التي يحيا البنك في كنفها، والتي لم يكن يعرفها العمل المصرفي من قبل. ويتناول البحث المعالجة القانونية لعلاقة البنك بموردي الأجهزة والبرامج اللازمة لإنشائه وتشغيله. وعلاقة البنك بمقدمي الخدمات الإلكترونية المسئولية عن تشغيله على شبكة الإنترنت، كما يعالج هذا البحث أيضا تنظيم علاقة البنك بجهة الرقابة المنوط بها الترخيص له بالإنشاء والعمل، مع التعرض لأهم المخاطر الرقابية المستجدة في عمل هذا البنك، والتي تحتاج إلى معاملة رقابية.

كما يتعرض هذا البحث لتنظيم القواعد التي تحكم التعاقد المصرفي على شبكة الإنترنت، من خلال التعرض لتعريف هذا التعاقد وإبراز أهم خصائصه، وقواعد إبرام العقد المصرفي على شبكة الإنترنت، وأهم العمليات المصرفية التي يمكن للبنك أن يقدمها على شبكة الإنترنت. وقد اهتم هذا البحث أيضا بتناول قضايا تأمين تواجد البنك ومعاملاته في ظل الطبيعة الأمنية الخاصة لشبكة الإنترنت، والتي أسفرت عن استحداث أشكال جديدة من الاعتداءات على البنك، بما استتبع

تغييرا في مفهوم أمن البنك، وآليات الحماية اللازمة لتأمينه، والمسؤولية القانونية عن هذه الاعتداءات.

وقد حرص هذا البحث عند تعرضه للقضايا القانونية التي يثيرها تنظيم إنشاء وعمل هذا البنك على استطلاع موقف القانون المصري، للنظر في مدى استيعاب القواعد القائمة لهذه القضايا، وإبراز أوجه القصور في هذا القانون من خلال مطالعة مواقف القوانين الأخرى في معالجة هذه القضايا، وتحليل مواقفها، والنظر في أكثر الحلول ملاءمة، وذلك من أجل أن نضع بين يدي المشرع المصري مقترحًا تنظيمًا دقيقًا لإنشاء وعمل هذا البنك.

ويجب ملاحظة أن طبيعة موضوع البحث اقتضت التعرض لبعض الجوانب الفنية الخاصة بإنشاء البنك وتشغيله على شبكة الإنترنت، وذلك بالقدر اللازم لخدمة البحث القانوني. ويأتي ذلك بهدف محاولة تقريب الرؤية قدر الإمكان عن طبيعة الأداءات الملقاة على عاتق أطراف التعامل، كي يكون التنظيم القانوني ملائما لواقع وطبيعة التزامات الأطراف.

هذا وقد حرص هذا البحث قدر الإمكان على تجنب التعرض للموضوعات التي لا تشكل إضافة جديدة؛ فمثلا لم يتعرض لتناول كافة العمليات المصرفية التي يمكن للبنك أن يقدمها، باعتبار أن القواعد القانونية المنظمة لهذه العمليات في البيئة التقليدية لن تختلف في نظام عمل البنك الإلكتروني على شبكة الإنترنت، واستعاض عن ذلك بتنظيم القواعد العامة التي تحكم إبرام كافة العقود المصرفية على شبكة الإنترنت. ثم اتبعنا ذلك بالتنظيم المفصل لبعض التطبيقات المصرفية كنماذج عملية؛خاصة تلك التي تعد من مستحدثات العمل المصرفي على شبكة الإنترنت؛ مثل إصدار النقود الإلكترونية، والتحويل الإلكتروني للنقود.

٢- أهمية موضوع البحث:

يشغل موضوع هذا البحث أهمية قصوى، تنطلق من ضرورة تبنى المشرع المصري لتنظيم قانوني يحكم وينظم عمل البنك الإلكتروني على شبكة الإنترنت. فالأخير لم يعد مجرد ترف اقتصادي يقتصر وجوده على الدول المتقدمة فقط، بل أصبح ضرورة لا غنى عنها لأي دولة، خاصة بعد اتفاقيات تحرير تجارة الخدمات(GATS)، وما حملته هذه الاتفاقيات في جعبتها من تحديات المنافسة فيما بين الدول، بات معه من اللازم، حتى تحتفظ هذه الدول بموقعها على الخريطة الاقتصادية العالمية، أن تستجمع المقومات المختلفة للمنافسة. ولاشك في أن البنك الإلكتروني وأنشطته المصرفية من أكثر المناطق التي تفرض تحديات كبيرة في هذا المجال في ضوء ما يقدمه من خدمات لا غنى عنها لأي نشاط تجارى.

ويأتى في مقدمة الخطوات التي يجب على مصر تخطوها على هذا الطريق تبنى تنظيم قانوني قوى يحكم إنشاء وتشغيل هذا البنك على شبكة الإنترنت، بنصوص دقيقة تراعى المتطلبات الخاصة لهذا البنك ولأنشطته المصرفية، ويجيب عن تساؤلات وقضايا أفرزها واقع هذا البنك، وباتت تلح في البحث عن الإجابة.

٣- مشكلة البحث:

تتلخص مشكلة البحث في أن وجود البنك الإلكتروني على شبكة الإنترنت أصبح أمرا واقعا لا مجال لإنكاره، يأتى ذلك في ظل غياب تنظيم تشريعى محدد من قبل المشرع المصري يحكم عمل هذا البنك، الأمر الذي شكل فراغا تشريعيا

في واحدة من أخطر المجالات تأثيرًا في الحياة الاقتصادية لأية دولة، وهو مجال البنوك ومعاملاتها المصرفية. وقد تسبب هذا الغياب التشريعى في العديد من المشاكل؛ أهمها؛ المحاولات المتكررة لثنى عنق النصوص القائمة لاستيعاب العلاقات المستجدة في نظام عمل البنك الإلكتروني. يضاف إلى ذلك أنفراد البنوك الالكترونية بتنظيم العقود التي تحكم تقديم خدماتها- باعتبار أنها الأقوى ـ وذلك على نحو عكس وجود تحكم وتعسف من قبل هذا البنوك بعملائها. وقد زادت وتيرة هذا الأمر بعد استحداث بعض الخدمات المصرفية التي ليس لها تنظيم قانوني مسبق.

وتعود هذه المشاكل في الأساس إلى التزاوج الذي تم بين البنك كتاجر يمارس أنشطة ذات طبيعة خاصة (الأنشطة المصرفية) وشبكة الإنترنت كوسيلة إلكترونية عالمية تتيح التعامل عن بعد، الأمر الذي انعكس على اختلاف مفهوم إنشاء وتشغيل البنك على شبكة الإنترنت عن مفهوم إنشاء وتشغيل البنوك التقليدية، بما طرح العديد من التساؤلات القانونية حول كيفية إنشاء البنك، وطبيعة علاقته بموردي الأجهزة الالكترونية والبرامج المعلوماتية؟

أيضا تسبب تواجد البنك على شبكة الإنترنت، وتعامله من خلالها في مشكلات حول طبيعة علاقته بمقدمي الخدمات الالكترونية (مقدم خدمة الدخول، مصمم الموقع الإلكتروني للبنك، متعهد الإيواء)، باعتبارهم من الوافدين الجدد على العمل المصرفي، وذلك للتعرف على مدى تأثر التزاماتهم بالطبيعة الخاصة للمعاملات المصرفية، خاصة البيانات التي قد يطلعون عليها بحكم عملهم، ومسؤولياتهم عما قد يقع من أضرار تلحق البنك أو المتعاملين معه؟

ترتب أيضا على اختلاف مفهوم إنشاء البنك الإلكتروني، والطبيعة الخاصة

للبيئة التي يعمل فيها (شبكة الإنترنت)، بروز تساؤلات تتعلق بأهمية الرقابة على إنشاء البنك وتشغيله على شبكة الإنترنت وذلك في ضوء طبيعة المخاطر التي تكتنف هذه الشبكة، والإجراءات الرقابية اللازمة للتأكد من استيفاء البنك للمعايير الكفيلة بمواجهة هذه المخاطر ومن ثم الترخيص له بالإنشاء والعمل؟

يطرح هذا البحث أيضا تساؤلات حول التعاقد بين البنك وعميله عبر شبكة الإنترنت، تتعلق بمفهوم هذا التعاقد، وأهم خصائصه، والالتزامات المصرفية المستجدة بفعل الطبيعة الالكترونية لشبكة الإنترنت، كوسيلة للتعاقد عن بعد. أيضا التساؤل عن أهم العمليات المصرفية المستحدثة في نظام عمل البنك الإلكتروني، وأهم الإشكاليات القانونية التي تطرحها هذه العمليات.

وأخير التساؤل عن مفهوم أمن البنك العامل عبر شبكة الإنترنت وصور الاعتداءات التي يمكن أن تخل بهذا الأمن ومسؤوليات المهاجمين عن هذا الإخلال، ومسؤولية الجهة المسئولة عن تأمين وجود البنك ومعاملاته في مواجهة البنك وعملائه؟

٤- صعوبات البحث:

- واجه هذا البحث العديد من الصعوبات، تمثلت أهمها في:

(١) قلة المصادر القانونية التي تناولت موضع البحث بالتنظيم. فلا يوجد تشريع مصري ولا عربي خاص يحكم عمل البنك الإلكتروني على شبكة الإنترنت، كما أن النظم القانونية الأجنبية التي عالجت هذا الموضوع عالجته بنصوص متناثرة، الأمر الذي استدعى محاولة حصر هذه النصوص قدر الإمكان. يضاف إلى ذلك أن أنشطة هذا البنك من الحداثة بمكان على النحو الذي

يصعب معه القول بوجود أعراف سائدة في هذا الخصوص. أيضا ندرة الأحكام القضائية التي تعرضت لمشاكل هذا البنك ومنازعاته.

(٢) قلة الدراسات القانونية المتخصصة التي تناولت هذا الموضوع بالبحث، بل أن هذه الدراسات القليلة تناولت بعض الجزئيات المتفرقة في نظام عمل البنك، كما أنها لم تراع آخر ما وصل إليه عمل هذا البنك من تطور.

(٣) الطبيعة الفنية لموضوع البحث. فالبنك الإلكتروني على شبكة الإنترنت عبارة عن مجموعة من الأجهزة والبرامج المترابطة فيما بينها والمتصلة بشبكة الإنترنت عن طريق موقع إلكتروني على هذه الشبكة، الأمر الذي استدعى التعرف عن قرب على هذه المسائل الفنية، وذلك في ظل عدم تخصص الباحث في هذه المسائل، مما دفع إلى الجلوس بين يدى المتخصصين في هذا المجال، بهدف الإلمام قدر الإمكان بهذه الجوانب الفنية لخدمة البحث القانوني.

٥- منهج البحث:

أنتهج الباحث في هذا البحث أكثر من منهج، وذلك على النحو التالي:

أ- المنهج التأصيلي:

دعت حداثة موضوع البحث إلى تناوله بمنهج تأصيلي، يسعى إلى رد الفروع إلى أصولها القانونية المستقرة في النظام القانوني المصري، وذلك من خلال النظر في مدى استيعاب هذه الأصول لما أفرزه عمل البنك الإلكتروني على شبكة الإنترنت من قضايا قانونية مستحدثة على العمل المصرفي، ومدى ملاءمتها لخصوصيتها في هذا الصدد فالبنك الإلكتروني في حقيقته بنك تجارى،

يقدم خدمات مصرفية، لكنه يعمل بطريقة إلكترونية، الأمر الذي دعا إلى ضرورة مراجعة القوانين الخاصة بعمليات البنوك، القوانين الرقابية السارية، والنظرية العامة للالتزامات المدنية والتجارية، وغيرها، للنظر في مدى ملاءمتها لما استجد في نظام عمل هذا البنك، وذلك قبل استطلاع موقف النظم القانونية التي تناولت هذا الموضوع بالتنظيم.

ب- المنهج التحليلي:

دعت الطبيعة الفنية لموضوع البحث إلى تبنى نظرة تحليلية للطبيعة الفنية لتكوين البنك وتعاملاته، وذلك من أجل فهم جيد لطبيعة الأداءات المختلفة للأفراد وطبيعة مسؤوليتهم عنها في ضوء المخاطر المرتبطة بها، ومن ثم إيجاد قالب قانوني مناسب يحكم وينظم علاقاتهم المختلفة، الأمر الذي دفع بالباحث في أوقات كثيرة إلى الجلوس على موائد المتخصصين فنيا في مجال نظم المعلومات والشبكات من أجل تقريب الرؤية وإيضاحها بنظرة قانونية متخصصة. من ناحية أخرى دعت قلة الدراسات القانونية في هذا المجال إلى تحليل نماذج العقود التي تحكم علاقات البنك المختلفة، سواء المتعلقة بمقدمي الخدمات الإلكترونية، أم تلك المتعلقة بعلاقته بعملائه، وذلك للنظر فيما يجرى عليه عمل هذه البنوك في الواقع، وتقييمه في ضوء قواعد العدالة والمنطق، خاصة في ظل ميل هذه البنوك إلى التخلي عن مسؤوليتها، وإثقال كاهل المتعامل معها بشروط غير عادلة، أيضا استعان البحث بالمنهج التحليلي فيما صدر عن القضاء من أحكام تعرضت لهذا الموضوع، وذلك للنظر في مدى مراعاة هذه الأحكام من خصوصيات عمل البنك الإلكتروني على شبكة الإنترنت.

ويعد كل من المنهجين التأصيلى والتحليلي من أكثر المناهج التي اعتمد عليهما

الباحث في هذه الدراسة، وذلك للأسباب السابقة.

ت- المنهج المقارن:

دعا غياب تنظيم قانوني مصرى إلى استشراف ما توصلت إليه النظم القانونية المختلفة من تنظيمات لهذا الموضوع، وذلك للتعرف على طبيعة الحلول التي تأخذ بها هذه النظم، والمقارنة فيما بينها، من أجل التوصل لأنسب الحلول ملائمة لطبيعة النظام القانوني للبنوك في مصر.

٦- خطة البحث:

ولتحقيق الغايات المرجوة من هذه الدراسة فقد اتبعنا خطة بحثية جرت على النحو التالي:

فصل تمهيدي:

المبحث الأول: تطور العمليات المصرفية الالكترونية.

المبحث الثاني:ماهية البنك الإلكتروني على شبكة الإنترنت.

الباب الأول: إنشاء البنك الإلكتروني على شبكة الإنترنت والرقابة عليه

الفصل الأول: إنشاء البنك الإلكتروني على شبكة الإنترنت.

المبحث الأول: التصميم الفني لشبكة البنك الإلكتروني والعقود اللازمة لذلك.

المبحث الثاني: عقود الخدمات الإلكترونية اللازمة لتواجد البنك على شبكة الإنترنت.

الفصل الثاني: الرقابة على البنك الإلكتروني على شبكة الإنترنت.

الالكترونى.

المبحث الثالث: المسؤلية المدنية لجهة التوثيق فى مواجهة البنك الالكترونى.

فصل تمهيدي

تطور العمليات المصرفية الالكترونية وماهية البنك الالكتروني

٧- تستهل هذه الدراسة معالجتها لموضوع البحث بتمهيد يتناول التطور الذي شهدته البنوك في تفاعلها مع وسائل الاتصال الإلكتروني وتكنولوجيا المعلومات، وذلك في محاولة لتقصي خطى التطور إلى أن وصل إلى حد وجود كامل للبنك على شبكة الإنترنت.

أيضًا دعا اختلاط وتداخل المفاهيم حول المقصود بالبنك الإلكتروني على شبكة الإنترنت إلى معالجة هذا الأمر، بتوضيح ماهية هذا البنك، وإبراز أوجه الاختلاف بينه وبين المفاهيم الأخرى التي تختلط معه، وتحديد طبيعته القانونية.

لذلك، نقسم هذا الفصل إلى مبحثين، الأول لمعالجة تطور العمليات المصرفية الإلكترونية والثاني لماهية البنك الإلكترونية على شبكة الإنترنت.

المبحث الأول

تطور العمليات المصرفية الإلكترونية

٨- تتميز عمليات البنوك بصورة عامة، والعمليات المصرفية الإلكترونية بصورة خاصة، بالتطور السريع والمستمر، ويعود ذلك أساسا إلى طبيعة البنك كتاجر يسعى دائما إلى تحقيق أقصى ربح ممكن من خلال جذب العملاء، الأمر الذي يدفعه إلى أن يترقب عن كثب ما يفرزه التطور التكنولوجي من معطيات، لتوظيفها في تقديم عملياته المصرفية. يساعد على ذلك ما تتمتع به هذه العمليات من قابلية عالية لاستيعاب التطورات في مجال تكنولوجيا المعلومات ووسائل الاتصال الإلكتروني. يضاف إلى ذلك أن فلسفة التشريعات المصرفية في الدول المختلفة راعت الاعتبارات السابقة، فظهر تدخلها لتنظيم العمليات المصرفية على استحياء، وعظمت من دور سلطان الإرادة في هذه العمليات، الأمر الذي أفسح المجال للبنوك كى تطور عملياتها بما يتماشى مع متطلبات العمل التجاري.

وقد سعت دول العالم ــ خاصة المتقدمة منها(١) – إلى تسخير مقدراتها الوطنية دعم البنوك في استفادتها من الوسائل الإلكترونية لتطوير عملياتها المصرفية.

---

(١) وقد كان من أهم هذه الدول: انجلترا والولايات المتحدة الأمريكية، وألمانيا وفرنسا وإيطاليا. وقد ظهر أثر ذلك فيما سعت إليه هذه الدول من تهيئة المناخ لاستفادة البنوك من وسائل الاتصال الإلكترونى، وذلك على كافة الأصعدة القانونية والاقتصادية والبنية التحتية لوسائل الاتصالات والمعلومات. أ. **المنصف قرطاس**، دراسة تحليلية حول فرص الاستثمار في البنك المباشر أو الانترنت البنكى، اتحاد المصارف العربية، ٢٠٠٠، ص ٢.

Apostolos Ath. Gkoutzinis, Internet banking and the law in Europe, Cambridge university press, First published, 2006, p 2

وقد اندفعت هذه الدول لذلك تحت تأثيرًا مجموعة من العوامل، أهمها:

- أن العمليات المصرفية هي الرابط والممول لكافة الأنشطة التجارية، في ضوء ما توفره من خدمات مالية وائتمانية لا غنى عنها لأي نشاط تجارى. وقد ازدادت أهمية هذا الدور في ظل الانفتاح الاقتصادي العالمي القائم على ثورة المعلومات وتكنولوجيا وسائل الاتصالات، حيث فرض هذا الانفتاح معطيات جديدة في ممارسة العمليات التجارية، الأمر الذي كان من اللازم معه أن تستجيب البنوك لهذه المعطيات، من خلال توظيف الوسائل الإلكترونية في تقديم عملياتها المصرفية، بما يجعلها ملائمة لواقع الممارسات التجارية.(١)

- يضاف إلى ذلك مزايا السهولة والسرعة والاقتصاد في النفقات التي يجنيها كل من البنك والعميل في ظل التعامل الإلكتروني؛ فقد ساعدت الوسائل الإلكترونية البنوك على التخفيف من غلواء البيروقراطية في العمل المصرفي، وذلك في ضوء ما تتيحه الوسائل الإلكترونية من حصول العميل على الخدمة المصرفية بعيدا عن التفاعل المباشر مع العاملين لدى البنك.(٢)

---

(١) **د. عدنان الهندى**، التجارة الإلكترونية والخدمات المصرفية والمالية عبر الانترنت، اتحاد المصارف العربية، ٢٠٠٠، ص١١

(2) **Susannah Fox and Jean Beier**, Online banking 2006: Surfing to the bank, Pew Internet & American life project, June 14, 2006, p 2; **Gautam Ivatury, Mark Pickens**, Mobile phone banking and low-income customers, Consultative Group to Assist the Poor/The world bank and United Nations Foundation, 2006,p 1; **Apostolos Kousaridas-George Parissis-Theodore ApostolOpoulos**, An open financial services architecture based on the use of intelligent mobile devices, Electronic commerce research and applications,

- اتساع ساحة المنافسة بين البنوك في ظل تجاذب أطراف العالم بفعل تقنيات الوسائل الإلكترونية، حيث تدافعت البنوك إلى اقتناص كل ما يفرزه التطور التكنولوجي من وسائل لتوظيفه في تقديم عملياتها المصرفية؛ لجذب أكبر عدد من العملاء وتحقيق أقصى ربح ممكن، وذلك في ظل ما يشهده قطاع الخدمات المالية من منافسة محتدمة ليس على النطاق المحلى فحسب، ولكن على النطاق الدولي أيضا(١)، فضلا عن أن المنافسة لم تعد محصورة بين البنوك فحسب، ولكنها امتدت لتشمل غيرها من المؤسسات المالية التي باتت تزاحمها في تقديم الخدمات المالية التي كانت بالأمس القريب حكرًا على البنوك(٢).

2007, p 233; **Olga Lustsik**, Can e-banking services be Profitable?, Tartu University press, 2004, p 18; **Everett Durante Cordy**, The legal regulation of e-commerce transactions, Journal of American Academy of Business, Cambridge; Mar 2003, p 400.

(1) **Sofia Giannakoudi**, Internet banking: The digital voyage of banking and money in cyberspace, Information & Communications Technology law, vol.8, No.3, 1999, p 205; **Jennifer Iser**, Across country analysis of the effects of E-banking and financial infrastructure on financial sector competition, Dissertation, School of business-Nova Southeaster university, 2008, p 62; **Rexnold Elias Byers**, Structuring service delivery processes: An examination of problems in retail banking and telephone center design, Dissertation, School of business administration, University of Rochester, 2000, p 9.

(٢) حيث ظهر اتجاه قوى من قبل بعض شركات التأمين والنفط والطيران والفنادق نحو تقديم خدمات الدفع الإلكتروني لعملائها، وذلك من باب التسهيل عليهم في التعامل معها. وقد تطلب هذا الأمر وجود حساب بنكي للعميل أو إجراء تحويل مالي من قبله، الأمر الذي يشكل منافسة تنطوي على كثير من المخاطر بالنسبة للبنوك.انظر: **يونس عرب**، مقالة بعنوان البنوك الإلكترونية، ص٥.

هذا وقد تميز استخدام البنوك للوسائل الإلكترونية في تقديم عملياتها المصرفية بعدة مميزات؛ أهمها:

- ♦ تباين استفادة البنوك من المعطيات المختلفة للوسائل الإلكترونية، متأثرة في ذلك بتباين قدرتها الفنية والمالية، وتباين الأعراف المصرفية السائدة، وتباين مواقف دول هذه البنوك في تبني تشريعات مصرفية تتلاءم مع هذا التطور، الأمر الذي أدى إلى تعدد أنماط العمليات المصرفية المقدمة.

- ♦ أن استفادة البنوك من الوسائل الإلكترونية في تعاملها مع العملاء ظهر بصورة تدريجية؛ حيث مكنت العميل في البداية من مجرد الحصول على الخدمة المصرفية بطريقة إلكترونية، وذلك بعد أن يكون التعاقد على هذه الخدمة قد تم في مقر البنك بطريقة تقليدية. ثم سعت البنوك إلى توسيع نطاق الاستفادة من الأدوات الإلكترونية ليشمل، ليس فقط مجرد تنفيذ الخدمة المصرفية، ولكن أيضا التعاقد على هذه الخدمة، وتنفيذ البنك لالتزاماته القانونية باستخدام هذه الأدوات(1).

- ♦ أن استفادة البنوك ظهر في اتجاهين: **الأول في** توظيف الوسائل الإلكترونية في تقديم عمليات البنوك التقليدية، والثاني في استغلال إمكانيات الوسائل الإلكترونية في استحداث عمليات مصرفية جديدة، تلبى احتياجات التجارة الإلكترونية.

٩- هذا وقد ترتب على استخدام البنوك للوسائل الإلكترونية في تقديم عملياتها المصرفية إلى ظهور مصطلح العمليات المصرفية الإلكترونية (Electronic

(1) **Apostolos Ath. Gkoutzinis**: Op. Cit, p. 7.

Banking)؛ كتعبير متطور وشامل للمفاهيم المتعددة التي ظهرت في أواخر القرن العشرين، والتي تشير في مجموعها للعمليات المصرفية الإلكترونية التي تتم عن بعد (Remote Electronic Banking).(١)

وقد عرفت هذه العمليات في تقرير لجنة بازل للبنوك الإلكترونية (١٩٩٨) بأنها عبارة عن الخدمات المصرفية صغيرة القيمة التي تقدم من خلال القنوات الإلكترونية.(٢)

وقد تم تعريفها أيضا من قِبل المجلس الأمريكي للرقابة على المؤسسات المالية الفيدرالية (FFIEC)(٣) بأنها عبارة عن تقديم الخدمات المصرفية الجديدة والتقليدية بصورة مباشرة للعملاء من خلال قنوات التسليم الإلكترونية التفاعلية، وذلك على نحو يمكن العملاء سواء كانوا أفرادًا أم شركات من الدخول للحساب والحصول على معلومات خاصة بالخدمات التي يقدمها البنك عبر الشبكات الخاصة أو العامة بما في ذلك شبكة الإنترنت(٤).

---

(1) **Jeanette Taft**; Op, Cit, p. 1; **Yoonhee Tina Chang**, Dynamics of internet banking adoption, ESRC centre for competition policy- University of East Anglia, ISSN 1745-9648, October 2005, p 4.**Money laundering**: A banker's guide to avoiding problems, (OCC),Second edition, 2002, p 15;**Reserve Bank of Australia**, Council of financial regulators annual report,2001,p14, available at:http://www.rba.gov.au/PublicationsAndResearch/CFRAnnualReports/2001/Pdf/cfr_annual_report_2001.pdf

(2) **Anita K. Pennathur, Clicks and bricks**: E-Risk management for banks in the age of the internet, Journal of internet banking and commerce (2001), p. 2105.

(3) (Federal Financial Institutions Examination Council).

(4) **E-Banking,** Federal financial institutions examination council, IT

كما عرفها البعض بأنها العمليات المصرفية التي تتم باستعمال الاتصال عن بعد سواء التليفون أم الإنترنت(١).

أيضا عرفت بأنها تقديم الخدمات المصرفية صغيرة القيمة عبر القنوات الإلكترونية (Electronic channels) (٢).

وعرفت كذلك بأنها الخدمات المصرفية التي تقدمها البنوك للعملاء في أي مكان وفى أي وقت، وتشمل الخدمات المصرفية المزودة عبر الهواتف الخلوية؛ مثل الخدمات المعلوماتية كالاستعلام عن الأرصدة والاطلاع على عروض المصارف وأسعار العملات والاستشارات والنصائح بشأن القروض والتسهيلات ومواقع البنك الفعلية ودوائره وغير ذلك من خدمات استعلامية، كما تشمل الخدمات المالية كتحويل النقود من حساب إلى حساب، وخدمات الدفع النقدي، وفتح الحسابات وغلقها، وغيرها من الأعمال والخدمات المصرفية(٣).

والملاحظ على مجموع هذه التعريفات أنها تنهل من معين واحد، وهو تقديم الخدمات المصرفية عن بعد عبر وسيلة إلكترونية، أي أن الأمر يتلخص في استخدام البنوك لبعض الوسائل الإلكترونية في تواصلها مع العملاء، مع احتفاظ

---

examination handbook, August 2003, p 1.

(١) **د.على أحمد مرسى عثمان**،العمليات المصرفية على الانترنت، مطبعة الصفا والمروة، ١٤٢٥هـ - ٢٠٠٤ م، ص٥٤.

(2) **G C CHALIKIAS**, A Guideline concerning electronic banking services- The case of Greece, MSc Thesis to school of industrial and manufacturing science-Cranfiled university, Academic Year 2003 –2004, p. 1.

(٣) راجع العنوان الإلكتروني التالي:

http://www.gamplus.com/app/wireless/technology/medex.htm

البنك بوجوده المادي وتعامله مع عملائه من خلال المقر المعروف به، على أن يكون العميل بالخيار بين أن يتعامل مع البنك في مقره بصورة تقليديـــة، أو أن يتعامل من خلال الوسائل الإلكترونية ليستفيد من المزايـــا التـــي تقـــدمها هـــذه الوسائل.

١٠- هذا وقد شهدت العمليات المصرفية الإلكترونية بالمفهوم السابق تعددا في أنماطها وأشكالها، وذلك لاختلاف وتنوع الوسائل الإلكترونية التي يعتمد عليهـــا البنك في تقديم خدماته للعملاء[١]، فـــي ضـــوء اخـــتلاف طاقتهـــا الاســـتيعابية والوظائف التي يمكن لها القيام بها[٢]. فالخدمات التي كان البنك يقدمها من خلال جهاز الصراف الآلي (ATM) تختلف عن الخدمات التي يقـــدمها مـــن خـــلال التليفون أو الكمبيوتر الشخصي للعميل (pc).

ومن أهم الأنماط التي ظهرت تطبيقا لذلك، جهاز الصراف الآلـــي، البنـــك المنزلي (Home Banking)، بنـــك الكمبيـــوتر الشخـــصي (PC-based E-banking)[٣]، وذلك على التفصيل التالي:

(١)- جهاز الصراف الآلي (Automatic Teller Machines):

يعد الصرف الآلي للنقود من خلال أجهزة الصرف الآلية الملحقة بالبنوك هي

---

(1) **Olga Lustsik**, Op. Cit, p. 19; **Gita Radhakrishna**, Liability issues in internet banking in Malaysia, International business information management association (IBIMA), 2009, p 1

(2) **Paola Garrone- Massimo G. Colombo**; Op. Cit, p. 539.

(3) **G C Chalikias**; Op. Cit, p. 2.

أولى أنماط العمليات المصرفية الإلكترونية[1]، والتي ظهرت في صورة أجهزة إلكترونية متصلة بالبنك، تعمل كنافذة خدمات يمكن للعملاء من خلالها الحصول على الخدمة المصرفية بواسطة بطاقة السحب النقدي (ATM Cards)[2]، حيث يتم إدخال هذه البطاقة في فتحة خاصة بها في ماكينة الصرف، ثم إدخال الرقم السري الخاص بهذه البطاقة، ثم طلب الخدمة المصرفية[3].

---

(١) وتعود النشأة التاريخية لهذه المكائن إلى عام ١٩٦٥ حيث تمت مقابلة بين مدير شركة (Dela Rue) وبين رئيس بنك باركليز، وانتهت إلى اتفاق مضمونه قيام شركة (Dela Rue) بتركيب ٥٧ ماكينة للبنك لصرف عشرة جنيهات إسترلينية في يوم عطلة البنك، وقد كان ذلك في فرع البنك بلندن. وفي الولايات المتحدة الأمريكية تم البدء باستخدام مكائن سحب النقود عام ١٩٦٩ (بداية عهد نظم التحويل الإلكتروني هناك) وكان ذلك من خلال منظمتي فيزا وماستركارد. وفي فرنسا كانت بداية ظهور هذه المكائن في بداية عام ١٩٧١. حيث قررت بعض البنوك الفرنسية وضع موزعات آلية للنقود لتمكين عملائها من الاستفادة من هذه الخدمة. انظر د. **منظور أحمد حاجي الأزهري**، بطاقة السحب النقدي، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون،٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص٣٦٠، انظر أيضا د. **كيلاني عبد الراضي محمود**، النظام القانوني لبطاقات الوفاء والضمان، دار النهضة العربية، ١٩٩٨م، ص ٩٣.

Jennifer Iser,; Op. Cit, p. 24.

(٢) وبطاقة السحب النقدي عبارة عن بطاقة ذات وجهين يبرز على الوجه الأول اسم الجهة المصدرة وعلامتها واسم حامل البطاقة ولقبه وغالبا صورته أيضا وتاريخ إصدار البطاقة ونهاية صلاحيتها ورقم البطاقة ورقم البنك في عضوية البطاقة (وهو رقم ثابت في كل البطاقات) والرقم المسلسل للبطاقة والرقم الخاص بعملية الإدخال على حاسب مركز البطاقات وتسجل البيانات المشفرة الخاصة بالحساب على الشريط الممغنط إلى جانب شريط آخر لتوقيع حامل البطاقة للتأكد من صحتها بالآلات الإلكترونية ويعطى العميل رقمًا سريًا خاصًا به يسمىpin . انظر د. **منظور أحمد حاجي الأزهري**،المرجع السابق، ص ٣٥٧.

(٣) لمزيد من التفصيل راجع د. **محمود سمير الشرقاوي**، مفهوم الأعمال المصرفية الإلكترونية وأهم تطبيقاتها. مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص ٤٤.

وقد مكنت مكائن السحب النقدي البنوك من تقديم العديد من الخدمات المصرفية الإلكترونية لعملائها، والتي من أهمها(1):

- إمكانية سحب النقود وإيداعها في هذه المكائن في أماكن تواجدها وفي أي وقت.
- إمكانية معرفة حالة الرصيد (دائن/مدين).
- إمكانية إجراء عمليات تحويل النقود من حساب لحساب آخر.
- إمكانية الحصول على دفتر شيكات .

هذا وقد تميزت الخدمات المصرفية المقدمة من خلال هذه المكائن بمجموعة من المزايا أدت إلى أنتشار استخدامها من قبل البنوك والأفراد بصورة كبيرة(2)، والتي من أهمها(3):

- **سهولة تقديم الخدمة المصرفية**؛ حيث يمكن للبنك تقديم الخدمة المصرفية

---

(1) **Roger Leroy Miller – Gaylord A. Jentz**, Law for e-commerce, West legal studies in business, 2002, p. 407, **Jennifer Iser**; Op. Cit, p. 32; **Sujit Chakravorti - Victor Lubasi,** Payment instrument choice: The case of prepaid cards, Economic Perspectives, federal reserve bank of Chicago, 2006, p. 31.

(2) وفقا للإحصاءات الصادرة عن بنك فرنسا في نهاية عام ١٩٩٠ فان عدد مكائن سحب النقود في فرنسا بلغ ١٤٨٢٨ ماكينة، وعدد العمليات المنفذة عن طريق هذه المكائن بلغ ٥٤٧,٧ عملية بقيمة ٢٤٢,٨ يورو. وفي ذات العام بلغ عدد المكائن لدى فيزا وماستركارد ٤٠٠ ماكينة تمت من خلالها ٦٠ مليون معاملة، وكان عدد الكروت الممغنطة ٢ مليون كارت. د. **منظور أحمد حاجى الأزهري**، المرجع السابق، ص ٦٠.

(3) د. **كيلانى عبد الراضي محمود**، المرجع السابق، ص ٩٧.

من خلال هذه المكائن بدون تدخل بشري، وفي وقت قصير وبعيدا عن ازدحام العملاء في مقر البنك وبتكلفة قليلة. كما يستطيع العميل عن طريق الضغط على مجموعة من **المفاتيح** المشفوعة بالبيانات والإرشادات من الحصول على الخدمة المطلوبة.

- **استمرارية تقديم الخدمة المصرفية**، حيث يستطيع البنك تقديم خدماته عبر هذه المكائن طوال أيام الأسبوع، وعلى مدار ٢٤ ساعة في اليوم، وذلك دون التقيد بأيام **عطلة البنك**، أو بساعات العمل اليومية.

- **اتساع نطاق تقديم الخدمة المصرفية**، حيث يمكن للبنك تقديم الخدمة عبر هذه المكائن ليس فقط في مقر البنك، ولكن في كل مكان تتواجد فيه هذه المكائن، حيث حرصت البنوك على نشر هذه المكائن في أماكن الخدمات المختلفة؛ كالمطارات والفنادق والمتاجر[١]. ليس هذا فحسب بل مكنت العميل من الاستفادة من هذه المكائن حتى ولو كانت تابعة لبنك آخر (غير الذي لديه حساب خاص به)، حيث جرت عادة البنوك بخصوص هذه الخدمات على أن تنشىء اتحادات تضم مجموعة من البنوك تقوم على إصدار هذه البطاقات، وتقبل التعامل بها من حامل البطاقة حتى ولو لم يكن عميلا لدى البنك الذي يطلب منه الخدمة. هذا من ناحية، من ناحية آخري استطاع البنك أن يوسع من دائرة نشاطه دون الحاجة إلى إنشاء فروع جديدة له، حيث تمثل كل ماكينة نافذة يقدم البنك خدماته من خلالها[٢].

وقد لعبت هذه المكائن دورا كبيرا في تعاملات البنوك، حيث استطاعت أن

---

(1) **G C Chalikas**; Op. Cit. p. 40.

(2) **Jennifer Iser**,; Op, Cit, p. 42.

تحقق جذبا كبيرا للعملاء، بواسطة المزايا الخاصة بهذه المكائن. وقد عملت البنوك على تأمين تقديم هذه الخدمة لعملائها من أجل كسب ثقتهم في التعامل معها[1]، وذلك بالحرص على الاستخدام الشخصي لهذه الوسائل من قبل العميل فقط؛ من خلال ربط التعامل معها بإدخال البطاقة الخاصة بالعميل وبإدخال الرقم السري، والتي هي بمثابة وسائل يستعين بها البنك للتحقق من شخصية العميل[2].

(٢)- العمليات المصرفية المنزلية (Home Banking):

تعرف العمليات المصرفية المنزلية بأنها عبارة عن "الخدمات المصرفية التي يمكن لعميل البنك الحصول عليها باستخدام التليفون أو التليفزيون أو الكمبيوتر الشخصي، عن طريق الاتصال بالكمبيوتر المركزي للبنك بشبكة خاصة "[3].

وعرفت أيضا بأنها عبارة عن تسليم الخدمات المصرفية عن بعد عبر وسيلة إلكترونية مثل التليفون[4].

وعرفت كذلك بأنها عبارة عن إجراء العمليات المصرفية والاستفسارات

---

(1); **Richard J. Sullivan**, Risk management and nonbank participation in the U.S. retail payments system, Federal reserve bank of Kansas city, P 6. available at: www.KansasCityFed.org. **Jennifer Iser**, Op, Cit, p. 50

(2) **Joris Claessens- Valentin Dem- Danny De Cock-Bart Preneel- Joos Vandewalle**, on the security of today online Electronic Banking System, Elsevier Advanced Technology, Vol. 21, No 3, p. 259; **Lucas D. Introna - Louise Whittaker**, Power, Cash, and Convenience: Translations un the political site of the ATM, Op, Cit, P. 332, 333.

(3) **G C Chalikias**; Op, Cit, p. 1.

(4) **Dictionary answers**, available at: http://www.answers.com/topic/online-banking

المعلوماتية عبر الكمبيوتر الشخصي(١).

وتعود فكرة العمليات المصرفية المنزلية إلى أوائل الثمانينيات(٢)، وذلك على أثر أنتشار استخدام الأجهزة الإلكترونية كالتليفون والكمبيوتر من قبل الأفراد نظرا لسهولة استخدامها، حيث سعت البنوك إلى استغلال ذلك في تواصلها مع العملاء. وقد كان لهذا الأمر تأثيرًا كبيرًا في جذب العملاء للتعامل معها، حيث كانت تتيح لهم إمكانية الحصول على الخدمات المصرفية من خلال المنزل أو مكتب العمل دون الانتقال إلى مقر البنك، وذلك على مدار اليوم(٣). لكن على الرغم من ذلك لم تحظ بذات القبول الذي حظيت به أجهزة الصراف الآلي(٤).

هذا وقد عملت البنوك على تطبيق العمليات المصرفية المنزلية في البداية عن طريق خطوط فردية خاصة للعملاء، بحيث يستطيع العميل الاتصال بالبنك عبر هذا الخط المتصل عنده بالتليفون أو بجهاز الكمبيوتر. ثم طورت البنوك هذه الوسيلة، عن طريق إنشاء شبكات خاصة(٥) تضم العملاء الذين يرغبون في

---

(1) **Shaoyi Liao- Yuan Pu Shao- Huaiqing Wang- Ada Chen**, Op. Cit, p. 68.

(2) **Jeanette Taft**; Op, Cit, p. 24.

(3) **Apostolos Ath. Gkoutzinis**, Op, Cit, p. 8.

(4) **Jeanette Taft**; Op, Cit, p. 26; **Shaoyi Liao- Yuan Pu Shao- Huaiqing Wang- Ada Chen**; Op, Cit, p. 68.

وقد يعود السبب من وجهة نظرنا وراء ما حظيت به أجهزة الصراف الآلي من انتشار أكبر من البنك المنزلي (Home Banking) إلى أن الأخيرة تعتمد على استعداد العميل، وذلك من خلال امتلاكه لمجموعة من الأجهزة الإلكترونية (كمبيوتر شخصي، تليفون) تمكنه من الاتصال بالبنك، الأمر الذي قد لا يتوافر للكافة. وذلك على عكس الحال بالنسبة لأجهزة الصراف الألي، والتي تتوقف على استعداد البنك من خلال إعداد هذه الأجهزة وإتاحتها للعملاء.

(٥) وهذه الشبكة الخاصة تعد من قبيل شبكات القيمة المضافة (**Value Added**

التعامل مع البنك من خلالها.

وقد كانت آلية الاتصال بين البنك والعميل تتم من خلال كود خاص بكل عميل، يستطيع من خلاله إرسال رسائل نصية بالخدمات التي يريدها، ثم ما لبث أن تطور هذا الأسلوب، حيث تم استعمال تقنيات تمكن العميل من التواصل بالصوت والصورة مع موظفي البنك (Video Conference). ولا شك أن هذا التطور قد انعكس على رضاء العملاء، وذلك لأنه أتاح فرصة أكبير للتفاعل والتواصل مع البنك، ليس فقط لمجرد الحصول على الخدمة المصرفية ولكن أيضا للتعاقد عليها عبر هذه الوسائل التي تسمح إمكاناتها بذلك(١).

أهم العمليات المصرفية المنزلية(٢):

١١- وتبدو أهمية التعرض لأهم العمليات المصرفية المنزلية، وذلك للتعرف على التطور الذي شهدته العمليات المصرفية الالكترونية في هذا النمط (العمليات

Networks)، التي تعرف بأنها عبارة عن شبكة اتصالات تعمل على ربط مجموعة من الشركاء التجاريين على نحو يسمح لهم بالاستفادة من خدمات الشبكة (مثل خدمة التبادل الإلكتروني للمعلومات)، بغض النظر عن القدرات الفنية والقياسية لكل شريك. وقد عملت العديد من البنوك على الاستفادة من مثل هذه الشبكات في التبادل الإلكتروني للبيانات المالية بينها وبين عملائها، وبينها وبين البنوك الأخرى. انظر. رأسم **سميح محمد عبد الرحيم**، التجارة الإلكترونية في خدمة التجارة والمصارف العربية (الجزء الأول)، اتحاد المصارف العربية، ١٩٩٧، ص١١٢ وما بعدها. انظر أيضا **إبراهيم المنجى**، عقد نقل التكنولوجيا، منشأة المعارف، الطبعة الأولى (٢٠٠٢)، ص ٢٨٠.

(1) **Paola Garrone- Massimo G. Colombo,** Op. Cit, p. 538.

(٢) رأفت رضوان، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، ١٩٩٨، ص ٦١.

-Available at: http://www.answers.com/tOpic/online-banking

المصرفية المنزلية). ومن أهم هذه العمليات:

- خدمات المعلومات (Information services)؛ والتي تتمثل في الاستفسار عن أية معلومات يريدها العميل خاصة بالخدمات التي يقدمها البنك، وشروط التعاقد الخاصة بها، والاستعلام عن أسعار العملات.
- خدمة الدخول إلى الحساب (Access to account)، وذلك لمعرفة حالته سواء كان دائنا أم مدينا.
- خدمات الدفع الإلكتروني (Electronic payments)، وهي خدمات تستهدف تسوية المبالغ المستحقة عن الصفقات بطريقة إلكترونية. وقد كان من أهم صورها نقل النقود بين حسابات العملاء إلكترونيا.

ويلاحظ بعد تعريف العمليات المصرفية المنزلية، والتعرض لأهم خدماتها أمران:

الأول: أن نظام العمليات المصرفية المنزلية يتميز عن نظام جهاز الصراف الآلي للنقود بأنه يتيح للعملاء الفرصة لمزيد من التفاعل مع موظفي البنك بخصوص الخدمات التي يقدمها البنك سواء في الاستفسار عن شروط هذه الخدمات أم في التعاقد والحصول عليها(١).

الثاني: أن فكرة العمليات المصرفية المنزلية تقتصر على استعانة البنك ببعض الوسائل الإلكترونية للتعامل مع العملاء، مع احتفاظه بكيانه المادي، وإمكانية

---

(١) المرجع السابق، ص ٥٩.

تقديمه لخدماته بصورة تقليدية من خلال هذا الكيان[1].

١٢- ويقتضي الحديث عن العمليات المصرفية المنزلية التعرض لأهم تطبيقات هذا النظام، وذلك على النحو التالي:

(أ)- الهاتف المصرفي Telephone banking:

يعد الهاتف المصرفي من أوائل صور الخدمات المصرفية الإلكترونية التي قدمتها البنوك لعملائها، حيث كانت تسعى من وراء ذلك إلى تمكينهم من إجراء بعض العمليات المصرفية البسيطة (التي تتناسب مع إمكانيات التليفون) دون الانتقال إلى مقر البنك[2].

ويجرى أسلوب العمل بنظام الهاتف المصرفي على أساس تقديم الخدمات المصرفية للعميل من خلال التليفون المنزلي أو من خلال شاشات إلكترونية خاصة بالعميل ومتصلة بمحطات طرفية تابعة للبنك[3]، حيث يعتمد العميل على استعمال لوحة المفاتيح الخاصة بالتليفون للاتصال بالبنك وإدخال الرقم السري الخاص به وطلب الخدمة المصرفية[4].

وهناك نوعان من تطبيقات الهاتف المصرفي، كما يلي[5]:

---

(1) **Shaoyi Liao- Yuan Pu Shao- Huaiqing Wang- Ada Chen**; Op. Cit, p. 68.

(٢) رأفت رضوان، المرجع السابق، ص ٥٨.

(3) **Gautam Ivatury, Mark Pickens**;Op, Cit, margin p. 1; **Apostolos Ath. Gkoutzinis**; Op. Cit, p. 8.

(4) **Joris Claessens- Valentin Dem- Danny De Cock-Bart Preneel-Joos Vandewalle**;Op, Cit, p. 253.

(5) **Shaoyi Liao- Yuan Pu Shao- Huaiqing Wang- Ada Chen**; Op,

الأول: نظام المشغل الحاضر (Operator-attended)، حيث يتيح هذا النظام للعميل الحصول على الخدمة المصرفية من خلال التخاطب المباشر مع موظف البنك. كما يتيح لموظف البنك الاستفسار عن الخدمة المطلوبة. وهذه الخدمة لا تكون متاحة طوال اليوم، حيث يحدد البنك للعميل الأوقات التي يمكن فيها الاتصال به(١).

الثاني: النظام الآلي (Automated)، حيث يتيح هذا النظام للعميل الاتصال بالبنك على مدار اليوم كله، ولكن الرد عليه من قبل البنك عن طريق الخدمات الصوتية المسجلة. ويتميز هذا النظام بأن الخدمات التي يمكن للعميل الحصول عليها بسيطة، كالاستفسار عن بعض المعلومات، كما يتميز بأنه أقل تكلفة من النظام السابق.

وقد حظي الهاتف المصرفي بأنتشار واسع في العديد من الدول لسنوات طويلة(٢). ويعود ذلك إلى إمكانية استخدامه في تقديم خدمات مصرفية عديدة،

Cit, p. 68.

(1) (WIZZIT provides customer support via a call center that is available 15 hours per day in the 11 official languages).
Gautam Ivatury, Mark Pickens; Op, Cit, margin p. 3.

(٢) ويعود ذلك إلى انتشار استخدام التليفون في هذه الدول، حيث تعد وسيلة الاتصال الأولى، حيث يقدر حجم مبيعات هذه التليفونات ب ٨٠٠ مليون تليفون في الفترة من ٢٠٠٤ -٢٠٠٦. يضاف إلى ذلك إمكانية الدخول للبنك عن طريقه من أي مكان. انظر:

Susannah Fox and Jean Beier, Online banking 2006: Surfing to the bank, Pew internet & American life Project, June 14, 2006, p. 2, **Shaoyi Liao- Yuan Pu Shao- Huaiqing Wang- Ada Chen**; Op . Cit, p 68

خاصة خدمات المعلومات(1)، وخدمات الدفع الإلكتروني (كسحب مبلغ معين من حسابه وتحويله على سبيل الوفاء ببعض الالتزامات الدورية التي يلتزم بها العميل كفاتورة الكهرباء، الغاز،التليفون)(٢) بصورة أكثر سهولة وبتكلفة أقل(٣).

وفي عام ١٩٨٦، تم إدخال خدمات إضافية للهاتف المصرفي؛ كتوضيح وشرح لعمليات التحويل التي يتم إجراؤها من قبل هذا العميل. وفي عام ١٩٩٤ طورت بعض البنوك(٤) هذه الخدمة، وذلك من خلال تمكين العميل من التعاقد للحصول على قرض من البنك(٥).

ويعد الهاتف المصرفي المنطلق الذي بدأ منه التطور بخصوص الخدمات المصرفية المنزلية، بل يمكن القول بأنه من أكثر الصور التي ظهرت عليها الخدمات المصرفية المنزلية، حيث كان العملاء يفضلون الاتصال بالبنك عن طريق التليفون دون غيره من الوسائل الأخرى كالكمبيوتر والتليفزيون. وهذا ما

---

(1) **Gautam Ivatury, Mark Pickens,** Op, Cit, p. 2.

(٢) ويستعين العميل غالبا لتنفيذ هذه العمليات ببطاقة للوفاء الإلكتروني (Debit Card)؛ انظر

Gautam Ivatury, Mark Pickens, Op, Cit, p. 2

(٣) فوفقا لبعض الدراسات التي أجريت في الولايات المتحدة الأمريكية تبين أن تكلفة إجراء العملية المصرفية عبر التليفون تقدر بـ ٤٠ % من تكلفة إجراء ذات العملية من مقر البنك.

Shaoyi Liao- Yuan Pu Shao- Huaiqing Wang- Ada Chen; Op, Cit, p. 64, **Gautam Ivatury, Mark Pickens,** Mobile phone banking and low-income customers evidence from South Africa, The world bank and United Nations Foundation, 2006, p.11.

(٤) ومن أمثلة البنوك التي قدمت هذه الخدمة لعملائها بنك **ميدلاند** وبنك **باركليز**. انظر رأفت رضوان، المرجع السابق، ص ٥٩

(5) **Jeanette Taft** ; Op, Cit, p. 27.

أكدته إحدى الدراسات المسحية التي أجريت في نيوزلندا عام ١٩٩٤ بخصوص نسبة اعتماد الأفراد على الأدوات التكنولوجية في إتمام المعاملات المصرفية، حيث أظهرت تفضيلهم استخدام التليفون بالمقارنة لغيره من الوسائط الأخرى(١).

(ب)- عمليات الكمبيوتر الشخصي PC –banking:

١٣- تجدر الإشارة، في البداية، إلى أن نظام عمليات الكمبيوتر الشخصي لا يقصد بها استخدام البنك للكمبيوتر في التعاملات المصرفية؛ كاستخدامه في تخزين البيانات واسترجاعها، أو الاعتماد عليه في العمليات المحاسبية والإحصائية، لكن يقصد بهذا النظام تواصل البنك مع عميله لتقديم الخدمات المصرفية على الكمبيوتر الخاص بالعميل والمتصل بالبنك عن طريق خط تليفوني أو شبكة خاصة(٢).

ويعتمد الحصول على عمليات الكمبيوتر الشخصي بهذا المعنى على استعانة العميل بمجموعة من الأدوات؛ وهى جهاز مودم (Modem) يثبت في الكمبيوتر الخاص بالعميل ومتصل بالبنك بخط اتصال (الذي هو عبارة عن خط تليفون)، ومجموعة من البرامج الخاصة المثبتة على جهاز الكمبيوتر الخاص بالعميل، مثل البرنامج المسئول عن عملية الاتصال بالبنك، وبرامج متخصصة في إجراء المعاملات المالية والمصرفية(٣). يضاف إلى ذلك احتفاظ العميل بكود خاص

(1) **Paola Garrone- Massimo G. Colombo**, Op. Cit, p. 539.

(2) **Shaoyi Liao- Yuan Pu Shao- Huaiqing Wang- Ada Chen**, , Op. Cit, p. 68.

(٣) **يونس عرب**، التعاقد والدفع الإلكتروني تحديات النظامين الضريبي والجمركي، ورقة عمل مقدمة لبرنامج الندوات المتخصصة حول التجارة الإلكترونية – معهد التدريب

التعريف به (Authentication password) عند اتصاله بالبنك (وعادة ما يقوم العميل بتسجيل هذا الكود على جهاز الكمبيوتر الخاص به، حيث أنه لا يتمكن من الاتصال بالبنك إلا عن طريق هذا الجهاز فقط). وغالبا ما يعتمد العميل في اختيار هذا الكود على بعض البيانات الخاصة به، مثل رقم الحساب(Account number)، ورقم التعريف الشخصي (Personal Identification Number)[1].

ويحظى نظام الكمبيوتر الشخصي بقبول واسع سواء من قبل الأفراد أم الشركات. ويعود ذلك إلى ما يتمتع به الكمبيوتر من إمكانيات تمكن من توجيه أوامر الدفع وإلغائها، وفحص الفواتير الخاصة بالمدفوعات والتحكم في كميات ومواعيد الدفع[2]. يضاف إلى ذلك إمكان الحصول على خدمات الإيداع المباشر[3]. وتبدو أهميته بالنسبة للشركات على وجه الخصوص، حيث تعمل على تحميل برامج محاسبية ذات قدرات فائقة في إتمام المعاملات المصرفية،

والإصلاح القانوني- الخرطوم، ٢٠٠٢، ص ٩.

(1) **Authentication in an Electronic Banking Enviroment**, Op. Cit, p. 2; **Sangjun Lee-SeungBae Park**, Mobile password system for enhancing usability-guaranteed security in mobile phone banking, springer- Verlag Berlin Heidelberg, 2005, p 67.

(2) **Brian Mantel,** Why don't consumers use electronic banking products? towards a theory of obstacles, Incentives and opportunities, Federal reserve bank of Chicago, 2000, p 26.

(3)**Tahir Masood Qureshi,** Customer acceptance of online banking in developing economies, Journal of internet banking and commerce, April 2008, vol.13, no.1,p14 available at: http://www.arraydev.com/commerce/jibc/

مما ادى إلى تبسيط إتمام هذه العمليات(١).

ووفقا للتقرير الصادر عن الهيئة الأوربية للرقابة على البيانات عـام ١٩٩٦ فأن نصف مليون شخص في أوربا يعتمد على الكمبيوتر الشخصي في التعامـل مع البنك، وكان يتوقع أن يصل هذا العـدد إلـى ٣ مليـون شـخص بحلـول عام٢٠٠١. وتعد ألمانيا وهولندا من أكثر الدول الأوربية اسـتعمالا للكمبيـوتر الشخصي(٢).

١٤- وبعد الانتهاء من عرض أهم صور العمليات المصرفية الإلكترونية، نبدى بعض الملاحظات عليها، وذلك على النحو التالي:

١- تدور جميع الصور السابقة في فلك فكرة واحـدة، وهـي تقـديم الخدمـة المصرفية عن طريق أحد القنوات الإلكترونية (مثل جهاز الصراف الآلـي، التليفون،، الشبكات الإلكترونية المغلقة)، لتسهيل التواصل مع العملاء وتقديم الخدمة المصرفية لهم، وذلك دون أن يتغير شكل البنك (كمبنـى لـه مقـر محدد)، فقط أصبح اتصال العميل بالبنك لطلب إحدى خدماته إلكترونيا.

٢- تقديم الخدمة المصرفية عبر الوسائل الإلكترونية يتناسب مع إمكانيات هـذه الوسائل، فكما أشارت التعريفات السابقة أنها خدمات مصرفية صغيرة القيمة أو بسيطة(٣)، بل يمكن القول أن هذه الوسائل تلجأ إليها البنوك، في الغالـب،

(1) **Katri kerem**, Internet banking in Estonia, Praxis center for Policy studies, 2003, p. 18.

(2) **Clara Cento**, Adoption of internet services in the acceding and candidate countries, (Lessons from the internet),Telematics and information, Vol 21,Issue 4, 2004, p 298

(٣) ومصطلح الخدمات المصرفية صغيرة القيمة يشير إلى العمليات المصرفية التي تـتم

لتلقي طلبات الخدمات المصرفية والرد عليها بصورة سهلة وسريعة، دون أن يكون المقصود تقديم كافة أنواع الخدمات المصرفية بالمعنى المألوف، وذلك بالنظر إلى الطاقة الاستيعابية لهذه الوسائل، وحجم وطبيعة الخدمات المصرفية.

٣- يتضح من الأنظمة السابقة أيضا أنها أنظمة مغلقة؛ بمعنى أن الاستفادة من الخدمات المصرفية الإلكترونية التي يقدمها البنك ليس متاحا للكافة، بل مقصور فقط على الأعضاء المشتركين في هذا النظام، حيث يحكم الاستفادة من هذه الخدمات نظام العضوية الذي ينظمه البنك بعقود تحكم وتنظم الانضمام إليه، الأمر الذي يتطلب ذهاب العميل أولا للبنك للتعاقد على الخدمة، على أن يتعامل عليها بعد ذلك إلكترونيا [١].

وإذا ما جاز لنا أن ننظر إلى الملاحظات السابقة على أنها أوجه للقصور، حيث شهدت تقنيات الأجهزة والبرامج وشبكات الإتصال تقدم لا يقبل معه قصر الاستفادة من الوسائل الإلكترونية على مجرد تواصل البنك مع عملائه بخصوص بعض العمليات المصرفية صغيرة القيمة. كما أظهرت ايضا قلة الخدمات المصرفية التي يستطيع العميل الحصول عليها بالنظر إلى الطاقة الاستيعابية للجهاز الإلكتروني الذي يعتمد عليه في الاتصال بالبنك، أو بإمكانية الاستفادة من

بخصوص صفقات تجارية بسيطة تتم بين الأفراد، أو المشروعات التجارية الصغيرة والمتوسطة، وهي مثل تسوية المدفوعات الخاصة بهذه الصفقات. انظر:

Adrian McCullagh and William Caelli, Internet banking: a matter of risk and reward, Springer-verlag berlin heidelberg, 2005, p 336

(1) **G C chalikias**; Op. Cit, p. 1.

هذه الخدمات باعتبار أن ذلك مقصور على الأعضاء فيها فقط.

١٥- لهذا سعت بعض البنوك إلى تحقيق أقصى استفادة ممكنة من الوسائل الإلكترونية لتقديم كافة أنواع الخدمات المصرفية التقليدية، وإلى استحداث خدمات مصرفية جديدة تتلاءم مع حاجات ومتطلبات التجارة الإلكترونية.

وقد وجدت هذه البنوك ضالتها المنشودة في العمل على شبكة الإنترنت[1]، هذا العمل لم يتمثل في مجرد استعمال البنك لشبكة الإنترنت في التواصل مع العملاء، ولكن في وجود كامل للبنك على شبكة الإنترنت، بحيث يحتوى موقعه على كافة البرمجيات اللازمة لأداء العمليات المصرفية. بل أكثر من هذا شهد العمل المصرفي تطورا جديدا في ظل عمل هذه البنوك؛ حيث لم يعد مقصورا على مجرد أداء خدمات مصرفية خاصة بحسابات العميل، بل أضيف إلى ذلك القيام بخدمات التسوق الإلكتروني والاستشارة المالية وخدمات الاستثمار والتجارة وغيرها[2]. وقد ساعد البنوك على كل هذا عدة عوامل، أهمها:

- إمكانات شبكة الإنترنت؛ من بساطة وسهولة في استخدامها من قبل الأفراد في أي وقت، ومن أي مكان[3]، يضاف لذلك اتساع نطاقها لتشمل العالم بأسره. كل ذلك دعا البنوك إلى تحقيق أقصى استفادة من هذه الإمكانيات، وتقديم خدمات مصرفية يحتاج إليها النشاط التجاري على شبكة الإنترنت[4].

---

(1) **Adrian mccullagh and William caelli**, Op. Cit, p. 340.

(2) **E-Banking,** Federal financial institutions examination council; Op. Cit, p. 5.

(3) **Shaoyi Liaoa and other**; Op. Cit, p. 64.

(4) **Richard J. Sullvan** How has the adoption of internet banking affected performance and risk in banks?, Federal reserve bank of

- التطور الهائل في تقنيات الحوسبة والبرمجيات، والذي ساعد بشكل كبير على ظهور أجيال قادرة على التبادل السريع والشامل للبيانات، بل ظهرت حاسبات وبرمجيات متخصصة في المعاملات المصرفية(١)، تتمتع بقدرات فائقة تسمح بتواصل العميل مع البنك عبر شبكة الإنترنت للاطلاع على الخدمات التي يقدمها والتعاقد بشأن هذه الخدمات وتنفيذها من قبل البنك(٢).

Kansas City, 2000, p 1.

(١) ويطلق على هذه البرمجيات برمجيات الإدارة المالية الشخصية (Personal-Financial-management PFM) وهي مثل (Microsoft's Money) وبرنامج (ntuits Quicken) وبرنامج (Meca's Managing Your Money) وغيرها. وترى مؤسسة الأبحاث الدولية أن البرامج الخاصة بالمعاملات المصرفية الإلكترونية كانت بمثابة الوصفة الجاهزة لمساعدة البنوك على التواجد والعمل على شبكة الانترنت. وقد قدرت نسبة مبيعات هذه البرامج عام ١٩٩٨ بـ ٩٣ مليون دولار، وفي عام ١٩٩٩ قدرت بـ ٣٢٦ مليون دولار.. انظر: **يونس عرب**، البنوك الإلكترونية، مرجع سابق، ص١.

Roger Leroy Miller – Gaylord A. Jentz, Law for e-commerce, West legal studies in business, 2002, p. 422.

(2) **Apostolos Ath. Gkoutzinis**; Op. Cit, p. 7.

المبحث الثاني

ماهية البنك الإلكتروني على شبكة الإنترنت

١٦- يكتسب تحديد ماهية البنك الإلكتروني على شبكة الإنترنت أهمية خاصة، مصدرها حداثة هذا النوع من البنوك، ووجود نوع من اللبس والخلط بخصوص ماهيته في ظل تعدد صور استفادة البنوك من الوسائل الإلكترونية في تقديم خدماتها المصرفية، خاصة شبكة الإنترنت، الأمر الذي يدعو إلى توضيح ماهية هذا البنك، من خلال وضع تعريف لهذا البنك، وإبراز أوجه الفرق بينه وبين الصور السابقة لاستفادة البنوك من الوسائل الإلكترونية، وتحديد طبيعة استخدام البنك لشبكة الإنترنت في التعامل مع العملاء، والتعرف على مدى اعتبار البنك الإلكتروني على شبكة الإنترنت بنكا من الناحية القانونية، وذلك على النحو التالي:

(١) تعريف البنك الإلكتروني على شبكة الإنترنت:

١٧- تجدر الإشارة إلى أن وضع تعريف محدد للبنك العامل على شبكة الإنترنت يثير صعوبة خاصة تتمثل في غياب نص تشريعي يقرب لنا رؤية واضحة لمفهوم هذا البنك. فعلى الرغم من أن ابتعاد المشرع عن صياغة التعريفات هو مسلك نشجع عليه، خاصة في بيئة دائمة التجدد والتطور كالبيئة التجارية بصورة عامة، والمصرفية بصورة خاصة، إلا أنه يبدو لنا أن هناك مسلكا وسطا نستطيع من خلاله تفادى صعوبات ضيق ألفاظ وعبارات النصوص وعدم استيعابها للفروض المتجددة، وفي ذات الوقت نضع رؤية واضحة للمقصود بهذا البنك لأهمية ذلك. هذا المسلك يتمثل في قيام المشرع بوضع

مجموعة من الخصائص التي تصاغ في صورة شروط يجب أن تتوافر حتى يمكن القول بأن هناك بنكًا إلكترونيًا يعمل على شبكة الإنترنت.

وتأتي الصعوبة السابقة في ظل أهمية وضع تعريف محدد للمقصود بالبنك الإلكتروني العامل عبر شبكة الإنترنت. هذه الأهمية تتجلى في الأسباب التالية:

- أن شبكة الإنترنت أتاحت الفرصة للعديد من المؤسسات والشركات التجارية لتقديم بعض صور الخدمات المالية، مثل خدمات الدفع الإلكتروني، وذلك بعد أن ساد الفكر لفترات طويلة بقصر القيام بهذه العمليات على البنوك فقط، الأمر الذي يدعو المشرع إلى ضرورة التدخل لوضع فواصل واضحة المعالم بين البنك الإلكتروني العامل عبر شبكة الإنترنت وغيره من الشركات التي تقدم بعض الخدمات المالية، وذلك لأن معظم النظم التشريعية المختلفة تفرد نظاما قانونيًا خاصا بالبنوك، ولا تسمح بسريان هذا النظام على مؤسسات أخري، سواء فيما يتعلق بإنشاء هذه البنوك (من تطلب رأس مال معين، وشكل قانوني خاص، أيضا بعض الإجراءات التي يجب أن تتبع)، أم ما يتعلق بالضوابط الرقابية الخاصة التي يجب أن تخضع لها هذه البنوك، وإجراءات تأمين خاصة بالعمل على شبكة الإنترنت(١). يضاف إلى ذلك أن الدول تنظر للبنك دائما على أنه عصب الاقتصاد القومي لديها، الأمر الذي

---

(١) وقد أكدت الاتفاقية الثانية للجنة بازل للرقابة على البنوك (٢٠٠١) هذا المعنى، حيث أشارت إلى ضرورة تحديد مفهوم الوحدة المصرفية بصورة دقيقة، وذلك حتى يكون إطلاق كلمة بنك خاضعا للرقابة، ومتطلبا التأكد من استيفاء معايير معينة من قبل السلطة المانحة للترخيص في ضوء توافر هذه المعايير من عدمه. د.**سهير محمود معتوق**، لجنة بازل وكفاءة الرقابة المصرفية، مجلة مصر المعاصرة (العدد ٤٨٢)، ٢٠٠٦، ص ٢٩.

يجعل هذه الدول تفرد البنوك بمعاملة خاصة؛ تهدف إلى تأكيد وتعزيز الثقة في التعامل معها؛ وذلك مثلا من خلال جعل الودائع لدى هذه البنوك مضمونة من قبل الدولة، الأمر الذي يدعو إلى ضرورة صياغة تعريف محدد للبنك الإلكتروني العامل على شبكة الإنترنت.

- أن البنوك اختلفت فيما بينها من حيث طريقة استفادتها من الوسائل الإلكترونية، خاصة شبكة الإنترنت في تقديم خدماتها كما سبق أن ذكرنا، وهذا الاختلاف يرتب تباينا في النظام القانوني الذي سيخضع له البنك في كل حالة(من حيث الإنشاء والرقابة ونظم التعاقد المصرفى)، الأمر الذي يدعو إلى ضرورة صياغة تعريف محدد للبنك الإلكتروني العامل على شبكة الإنترنت، وذلك منعا لللبس.

- أن شبكة الإنترنت وتقنيات الحوسبة والبرمجيات المتخصصة أتاحت للبنك العامل على هذه الشبكة أن يقدم إلى جوار الخدمات المصرفية التقليدية طائفة من خدمات المعلومات والخدمات التسويقية، التي تعد حديثة العهد بالعمل المصرفى، الأمر الذي يحتاج إلى تحديد مفهوم واضح لهذه البنوك من أجل النظر فيما إذا كان القانون ينظر إليها في ظل هذه البيئة الجديدة على أنها بنك بالمفهوم القانوني المعروف أم لا.

وفي ظل أهمية هذه الأسباب، وفي ظل الصمت التشريعي فيما يتعلق بتعريف هذه البنوك، وجد الفقه المجال رحبا كي يدلي كل بدلوه لتعريف البنك الإلكتروني العامل على شبكة الإنترنت، الأمر الذي ترتب عليه جعل كل واحد من الفقهاء يعرف البنك من زاوية خاصة به.

وقد تعددت الأسماء التي أطلقها الفقهاء على هذا البنك؛ فالبعض يطلق عليه بنك

الإنترنت (Internet Bank) [١]، والبعض يطلق عليها بنك الويب (Web Bank) [٢]، والبعض يطلق عليه البنك الافتراضي(Virtual bank) [٣].

١٨- هذا وقد تعددت الاتجاهات التي تناولت هذا البنك بالتعريف إلى ثلاثة اتجاهات، حيث نظر كل اتجاه لهذا البنك من زاوية معينة، غافلا عن الزوايا الأخرى، وذلك على النحو التالي:

الاتجاه الأول: تقديم بعض الخدمات المصرفية على الانترنت

عرف أحد أنصار هذا الاتجاه البنك الإلكتروني على شبكة الإنترنت بأنه " البنك الذي يقدم الخدمات المصرفية عبر الموقع الإلكتروني له على شبكة الإنترنت" [٤].

وعرف أيضا بأنه " البنك الذي يسمح موقعه للعملاء بإجراء التحويل الإلكتروني للنقود على الأقل" [٥].

وعرف كذلك بأنه عبارة عن "موقع إلكتروني يقدم الخدمات المالية في البيئة الافتراضية" [٦].

---

(1) **Jaakko Vilén**, Accessibility in internet services–case electronic banking, Master's thesis, Hesnkil university of technology, available at : lib.tkk.fi/Dipl/2006/urn007525.pdf

(٢) انظر: يونس عرب، البنوك الإلكترونية، مرجع سابق، ص ١.

(3) **Shaoyi Liaoa and other**; Op. Cit, p. 63.

(4) **Richard J. Sullvan** ; Op .Cit, p. 3.

(5) **Ibid.**, p. 15.

(6) **Jeanette Taft**, An examination of the antecedents of electronic banking technology acceptance and use, Dissertation, Faculty of the College of business administration Of Touro University

ويبدو لنا أن هذا الاتجاه منتقد من نواح عدة:

أ- أنه يفتح المجال للخلط بين الأنماط المختلفة لاستفادة البنوك من شبكة الإنترنت، فكما سبق أن ذكرنا أنه ليس كل موقع الكتروني لبنك على شبكة الإنترنت يمكن معه القول إننا بصدد بنك إلكتروني يعمل على شبكة الإنترنت.

ب-أن هذه التعريفات قصرت الخدمات التي يقدمها البنك على الخدمات التي تتم على شبكة الإنترنت فقط، رغم أن وجود البنك على شبكة الإنترنت يجعل الفرصة أمامه مواتية لتقديم خدمات تسويقه وخدمات استثمارية.

ج- هذه التعريفات ذات طابع فني بحت، وتغفل معالجة الجانب القانوني للبنك.

الاتجاه الثاني: مجرد التواجد على الانترنت

عرف أنصار هذا الاتجاه البنك الإلكتروني على شبكة الإنترنت بأنه " البنك الذي يتواجد فقط على شبكة الإنترنت"(١).

وعرفه أيضا أحد القواميس الالكترونية المتخصصة بأنه " البنك الذي يتواجد فقط على شبكة الإنترنت من خلال شبكة داخلية متصلة بشبكة الإنترنت"(٢).

---

international, October 24, 2007, p. 30.

(1) **G C Chalikias**; Op. Cit, (Glossary)

انظر أيضا الموقع الإلكتروني التالي:

http://www.gamplus.com/app/wireless/technology/mdex.htm

(2) **All Business**, Business Glossary, available at:

وعرف كذلك بأنه عبارة عن " البنك الذي يعمل فقط على شبكة الإنترنت"[1].

وعلى الرغم من تفادى هذا الاتجاه النقد الذي وجه للاتجاه السابق؛ وذلك بخصوص الخلط بين الأنماط المختلفة للبنوك، إلا أنه منتقد في أمرين:

(١) قصر تقديم البنك الإلكتروني لخدماته فقط على شبكة الإنترنت. فعلى الرغم من أن هذا البنك لا يعمل إلا على شبكة الإنترنت إلا أنه يمكن أن يؤدى خدماته في البيئة الواقعية من خلال مكائن السحب الآلي وبطاقات الدفع الإلكتروني المختلفة.

(٢) أن هذا الاتجاه أورد تعريفات فنية تغفل الجوانب القانونية.

الاتجاه الثالث: عدم الوجود المادى للبنك

عرفه هذا الاتجاه بأنه "البنك الذي ليس له فروع مادية ويؤدى خدماته عبر شبكة الإنترنت وجهاز الصراف الآلى"[2].

عرف كذلك بأنه عبارة عن " البنك الذي ليس له فروع مادية، والذي يتواصل مع عملائه عبر وسائل إلكترونية متصلة بشبكة الإنترنت؛ كجهاز الصراف الآلي

---

http://www.allbusiness.com/glossaries/ virtual-banking/4942088-1.html

(1) The free dictionary, available at: http://financial-dictionary.thefreedictionary.com/Virtual +bank

(2) **Informix provides server for virtual bank. (Security First National online bank will use database server from Informix),** available at:
http://www.highbeam.com/doc/1G118760462.html

(ATM) والتليفون والكمبيوتر الشخصي[1].

وعلى الرغم من أن هذا الاتجاه قد تفادى إنتقادات التعريفات السابقة، إلا أنه أغفل الجانب القانونى.

ويمكن لنا أن نعرف هذا البنك بأنه عبارة عن موقع إلكتروني على شبكة الإنترنت يحتوى على كافة البرمجيات اللازمة للتعامل بصورة كاملة مع العملاء بخصوص الخدمات المصرفية وغيرها من الخدمات التسويقية ويرخص له القانون بممارسة أنشطته في بيئة إلكترونية.

١٩- ومن هذا التعريف يمكن الوقوف على أهم الخصائص التي يجب أن تتوافر في البنك العامل عبر شبكة الإنترنت، وهي:

أ- البنك الإلكتروني العامل عبر شبكة الإنترنت ليس له كيان مادي ملموس (Non-branch bank)، بل هو عبارة عن موقع إلكتروني على شبكة الإنترنت يحتوى على كافة البرمجيات اللازمة للتعامل بصورة كاملة مع العملاء بخصوص الخدمات المصرفية.

ب-يقدم البنك الإلكتروني العامل على شبكة الإنترنت مجموعة متكاملة من الخدمات المصرفية عبر موقعه الإلكتروني على شبكة الإنترنت، ولا يقتصر الأمر على مجرد الإعلان عن الخدمات المصرفية للعملاء عبر هذا الموقع.

ج- الحصول على ترخيص قانوني من الجهة المخولة بذلك لتقديم الخدمات المصرفية على شبكة الإنترنت.

---

(1) **Shaoyi Liaoa and other**; Op. Cit, p. 63.

ويعد بنك (Netbank) [1] هو أول بنك إلكتروني عامل على شبكة الإنترنت بالمفهوم السابق، وكان ذلك في عام ١٩٩٥[2].

٢٠- وتجدر الإشارة إلى أن البنك العامل على شبكة الإنترنت بالمفهوم السابق يمكن أن يظهر على صورتين[3]:

الأولى: وهى ألا يكون للبنك أي فروع مادية، بمعنى أنه لا وجود للبنك إلا على شبكة الإنترنت، من خلال موقعه الإلكتروني على هذه الشبكة

---

(١) هذا البنك موجود على العنوان الإلكتروني التالي:

www.netbank.com

(٢) انظر: **يونس عرب**، البنوك الإلكترونية، مرجع سابق، ص ٩.

- وهذه البنوك في زيادة مستمرة وتشهد استقطابًا واسعًا للمتعامين معها. ففي الولايات المتحدة الأمريكية بلغ عدد عملاء هذه البنوك ٤٤ مليون عميل عام ٢٠٠٦ وهذا العدد في تزايد حيث تفوق نسبة زيادة العملاء نمو شبكة الانترنت ذاتها. ويوجد حوالي ٧ ملايين شخص في أستراليا يتعاملون مع البنوك الإلكترونية العاملة عبر شبكة الانترنت. وفي تركيا قدر أن ٢٠% من مستخدمي الانترنت يتعاملون مع البنوك الإلكترونية العاملة عبر شبكة الانترنت، وأن عدد المتعاملين في زيادة مستمرة. وفي المملكة المتحدة زاد عدد المستخدمين لهذه البنوك بنسبة ٥٠% عما كان عليه الحال في ٢٠٠٥.

- ومن أهم البنوك الإلكترونية العاملة عبر شبكة الانترنت:

, Network Bank, KevCorp Republic Bank & Trust Bank One, USAccess Bank

First National Bank of the Internet , First Internet Bank , NationsBank, Bank of New York

Adrian McCullagh -William Caelli,; Op. Cit, p. 336: **Rob Rachwald**, Is banking online safer than banking on the corner?, Online banking, Computer fraud & Security, 2008, p. 11: **Katri kerem**,; Op. Cit, p. 19.

انظر أيضـ **يونس عرب**، البنوك الإلكترونية، مرجع سابق، ٧.

(3) **Shaoyi Liaoa and other**, Op. Cit. p. 63.

الثانية: هي أن يكون للبنك فروع مادية، لكن لا يتعامل من خلالها.

(٢) مظاهر اختلاف البنك العامل على شبكة الإنترنت والبنوك المقدمة للخدمات الإلكترونية:

٢١- تجدر الإشارة بداية إلى أن البنك الإلكتروني على شبكة الإنترنت لا يخرج عن مفهوم البنوك المقدمة لخدمات مصرفية إلكترونية بالمعنى الذي سبق أن تعرضنا له، من حيث كونه بنكا يقدم الخدمات المصرفية عن بعد عبر وسيلة إلكترونية. لكن هذا لم يمنع من وجود بعض أوجه للاختلاف، أهمها:

أ) البنك الإلكتروني على شبكة الإنترنت ليس له كيان مادي ملموس (Non-branch bank). بل هو عبارة عن شبكة إلكترونية متصلة بموقع إلكتروني على شبكة الإنترنت، تحتوى على كافة البرمجيات اللازمة للتعامل بصورة كاملة مع العملاء بخصوص الخدمات المصرفية، بداية من الإعلان عن الخدمة المصرفية، ومرورا بالتعاقد عليها، وانتهاءً بتنفيذ هذا العقد[١]. أما البنوك المقدمة لخدمات مصرفية الكترونية فهي بنوك تقليدية، ذات كيان مادي، تتواجد في عنوان معروف، وتسمح بالتعامل مع العملاء عبر هذا الكيان، لكنها تقدم بعض الخدمات المصرفية في صورة إلكترونية بغرض التسهيل على عملائها والاقتصاد في نفقات هذه الخدمات.

ب) يقدم البنك الإلكتروني على شبكة الإنترنت كافة الخدمات المصرفية التي تتناسب مع طبيعته الالكترونية[٢]، بالإضافة إلى ما يوفره لعملائه من فرصة

(1) **Ibid**, p. 63.

(2) **G C Chalikias**; Op, Cit, p. 38; **Katri kerem**; Op. Cit, p. 23.

كبيرة في الاختيار بين البدائل المصرفية المتعددة، وذلك بفضل التصميم الفني لشبكة البنك، والتي تحتوى على مجموعة من الأجهزة والبرمجيات التي تمكن البنك من ذلك(١)، أما الوضع بالنسبة للبنـــوك المقدمـــة لخـــدمات مـــصرفية إلكترونية، فأن الأمر يقتصر على مجرد صور بسيطة للتعامـــل المـــصرفى؛ كإدارة الحساب المصرفي، أو إرسال طلبات للحصول على بعض الخـــدمات المصرفية، التي تتناسب مع قدرات وسيلة الاتصال الإلكترونية بـــين البنـــك والعميل.

ت) البنك الإلكتروني على شبكة الإنترنت على الرغم من اعتماده القوى علـــى الكمبيوتر الشخصي والتليفون المحمول وجهاز الصراف الآلي للتعامـــل مـــع عملائه (باعتبارها أدوات قادرة على الاتصال بشبكة الإنترنت)، إلا أنـــه لا يتماثل في ذلك مع البنوك المقدمة لخدمات مصرفية إلكترونية؛ حيـــث فـــي الحالة الأولى (البنك العامل على الإنترنت) البرمجيات المسئولة عن التعامـــل المصرفي موجودة على الموقع الإلكتروني للبنك، ومن ثم يـــستطيع العميـــل التعامل معه من أي جهاز كمبيوتر أو تليفون جهاز صراف آلي، بـــشرط أن يكون متصلا بشبكة الإنترنت، الأمر الذي يوسع من فرصة تعامل العميل مع البنك من أي مكان(٢). أما في الحالة الثانية (البنوك المقدمة لخدمات مصرفية

---

(1) **Fethi Calisir- Cigdem Altin Gumussoy**, Internet banking versus other banking channels: Young consumers' view, International Journal of Information Management (Science Direct), 2008, p. 215.

(2) **Shaoyi Liaoa and other**; Op. Cit, p. 69; **Internet banking services - virtual bank**, available at: http://www.clearleadinc.com/site/internet_banking.html

الكترونية)، فأن البرمجيات المسئولة عن المعاملات المصرفية موجودة فقط في جهاز الكمبيوتر الخاص أو في تليفون العميل، ومن ثم لا يستطيع التعامل مع البنك إلا من خلال أحد هذه الأجهزة.

ث) يتميز البنك الإلكتروني على شبكة الإنترنت بأن موقعه ليس مجرد نافذة يقدم من خلالها الخدمات المصرفية فحسب، بل يقدم أيضا بعض الخدمات التسويقية؛ حيث يستضيف على موقعه الإلكتروني وصلات خاصة بمتاجر إلكترونية تعرض سلعا ومنتجات، أو مواقع خاصة بتداول الأسهم، أو مواقع تقدم خدمات السمسرة، وخدمات الشحن والسفر، وذلك ضمن مفهوم الخدمة الشاملة (وقفة التسوق الواحدة One – stop shopping)[١] التي تساعده على جذب العميل، وذلك على عكس الوضع بالنسبة لأنماط البنك الإلكتروني الأخرى التي لا تقدم هذا المفهوم من الخدمات، وذلك بالنظر إلى إمكانيتها الضعيفة بالمقارنة بالبنك العامل عبر شبكة الإنترنت.

وبعد تعريف البنك الإلكتروني على شبكة الإنترنت، وإبراز أهم أوجه الاختلاف بينه وبين البنوك المقدمة للعمليات المصرفية الالكترونية، يثور تساؤلا،

---

(١) وتقوم فكرة الخدمة الشاملة أو وقفة التسوق الواحدة على أساس احتفاظ البنك بعميله وإبقائه على موقعه، وذلك من خلال توفير كل الخدمات التسويقية (سلع وخدمات) المتصلة بالخدمة المصرفية. ويتم ذلك إما عبر شركات تابعة للبنك أو عن طريق جهات خارجية ترتبط بموقع البنك عبر وصلات مرتبطة بموقع البنك وتكفل عودة العميل مرة آخري لموقع البنك لإتمام العملية المصرفية المرتبطة بالخدمة غير المصرفية.وهذا ما يمثل مفهوم البنك الإلكتروني الشامل، والذي يطلق عليه بعض الباحثين عبارة وقفة التسوق الواحدة. انظر: **يونس عرب**، البنوك الإلكترونية، مرجع سابق، ص ٢؛ رأفت رضوان، عالم التجارة الإلكترونية، مرجع سابق، ص٦٢.

Martin Sloan, Web accessibility and the DDA, Journal of Information law and technology. 2001, p 27

هل كل بنك يتواصل مع عملائه عن طريق شبكة الإنترنت يعد بنكا إلكترونيا يعمل على شبكة الإنترنت؟

تبدو لهذا السؤال أهمية خاصة؛ حيث تسود العديد من المفاهيم الخاطئة في تحديد مفهوم البنك الإلكتروني على شبكة الإنترنت، وذلك على أثر تعدد طرق استعمال البنوك لشبكة الإنترنت. فليس كل ظهور لبنك على شبكة الإنترنت يعنى أنه بنك إلكتروني يعمل على هذه الشبكة. ومن ثم تقتضى الاجابة على هذا السؤال التعرف على طبيعة استفادة البنك الإلكتروني من شبكة الإنترنت.

(٣) طبيعة استفادة البنك الإلكتروني من شبكة الإنترنت:

٢٢- تتعدد صور استفادة البنوك من شبكة الإنترنت، وذلك على النحو

- الموقع المعلوماتي Informational Site:

وتقوم فكرة الموقع المعلوماتي على أساس قيام البنك التقليدي بإنشاء موقع إلكتروني على شبكة الإنترنت لمجرد الإعلان والتعريف بخدماته وفروعه، دون أن يكون هناك أي معاملات تبادلية مع عملائه عبر هذا الموقع(٢). وهذا بالطبع

---

(1) **Internet Banking**, Comptroller handbook, Comptroller of the currency administrator of national banks , October 1999, p. 4.: **Is auditing guideline internet banking**, Information systems audit and control association, document G 24, 2003, p 2, Available at: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=18637

- انظر أيضا **يونس عرب**، البنوك الإلكترونية، مرجع سابق، ص ٣.

(٢) ويوجد مجموعة من البنوك تكتفي بهذا التواجد على شبكة الانترنت، ومن أشهر هذه

لا يقصد بالبنك الإلكتروني العامل عبر شبكة الإنترنت.

- الموقع الاتصالى Communicative Site:

ويقصد بالموقع الاتصالى قيام البنك التقليدي بالتواصل مع عملائه بخصوص بعض الخدمات المصرفية التي يقدمها، وذلك من خلال موقعه على شبكة الإنترنت، فالبنك في هذه الصورة يعتمد على شبكة الإنترنت كبديل عن وسائل الاتصال الأخرى (كالتليفون، أو الكمبيوتر المتصل بخط خاص) للتواصل بالعملاء؛ كاستلام رسائل البريد الإلكتروني الخاصة ببعض الخدمات المصرفية التي يريدها العميل، أو أن يقوم العميل بملء نماذج طلبات لبعض الخدمات، أو الاطلاع على المعلومات الخاصة بحسابه المصرفي(1). وذلك مع احتفاظ البنك بكيانه المادي، وتقديمه لخدماته من خلاله. وهذه الصورة تسمى بالأعمال المصرفية على شبكة الإنترنت (Internet Banking). وتعرف هذه الصورة بأنها عبارة عن "استخدام شبكة الإنترنت كوسيلة تسليم إلكترونية عن بعد لبعض الخدمات المصرفية، والتي تتضمن الخدمات التقليدية؛ مثل فتح حساب أو إجراء تحويل للنقود بين حسابين مختلفين، هذا بالإضافة لبعض الخدمات الجديدة مثل الدفع الإلكتروني للفواتير عبر شبكة الإنترنت(2)" كما عرفت أيضا بأنها عبارة عن عبارة عن تقديم الخدمات المصرفية الإلكترونية عبر شبكة الإنترنت عن طريق الكمبيوتر الشخصي (PC) أو الأدوات الإلكترونية الأخرى القادرة على

البنوك في آسيا (Wing Hang Bank)، (Dao Hang Bank)، (International Bank).

Shaoyi Liaoa and other;Op. Cit, p. 69.

(1) **G C Chalikias**, Op. Cit, p. 38.

(2) **Is auditing guideline internet banking; Op.** Cit, p. 2.

الاتصال بالإنترنت(١).

ويعد البنك الرئاسي في مارى لأند Presidential Bank of Marylandباستراليا هو أول بنك يقوم بتطبيق فكرة الموقع الاتصالي وقد كان ذلك في أكتوبر عام ١٩٩٥، بعد ذلك بقليل تبعه بنك فارجو Fargo Bank في عام ١٩٩٦، ومنذ ذلك الحين بدأت البنوك تتوالى في الظهور على شبكة الإنترنت(٢).

وهذه الصورة لا تمثل المقصود بالبنك الالكتروني على شبكة الإنترنت؛ حيث إن البنوك في هذه الصورة تلجأ لاستخدام شبكة الإنترنت من باب التسهيل على العملاء بخصوص بعض الخدمات المصرفية، مع احتفاظ البنك بمقره التقليدي والاعتماد عليه بشكل أساس في التعامل مع العملاء. هذا وأن كانت هذه الصورة تعد أقرب الصور للبنك العامل على شبكة الإنترنت.

- الموقع التفاعلي Transactional Site(٣):

يمكن هنا القول بأننا بصدد بنك إلكتروني يعمل على شبكة الإنترنت، حيث يظهر البنك في هذه الصورة بموقع إلكتروني متصل بشبكة إلكترونية داخلية

---

(1) **Apostolos Ath. Gkoutzinis**;Op, Cit, p. 8.

(2) **Adrian McCullagh and William Caelli**; Op. Cit, 338.

(٣) ويطلق على هذا النوع من المواقع أيضا الموقع النشط (**Active web site**)، حيث يستمد هذا الاسم من قدرة هذا الموقع على التفاعل مع الأفراد بخصوص التعاقد والحصول على السلع والخدمات محل التعاقد عبر الموقع. بينما يطلق على الموقع الذي لا يوفر هذه الإمكانيات، ويقتصر دوره على مجرد الإعلان عن الخدمات اسم الموقع الخامل أو السلبي **(passive web sites)**.

Lorna Gillies, Jurisdiction for consumer contracts, Computer law & Security report Vol. 17 no. 6 2001, p 397.

مزودة بكافة البرمجيات التي تؤهله للقيام بكافة العمليات المصرفية لعملائه عبر شبكة الإنترنت[١]، ودون أن يكون له فروع مادية (Non-branch Bank)[٢]، حيث يمكن للعميل من خلال الاتصال بشبكة الإنترنت عبر أية وسيلة إلكترونية(جهاز الصراف الآلي ATM، التليفون المحمول Mobile Phone، الكمبيوتر PC) إجراء كافة المعاملات المصرفية من فتح حساب مصرفي وإجراء عمليات إيداع وسحب من هذا الحساب،.وإجراء الدفع الإلكتروني، وإجراء التحويلات النقدية، والحصول على كافة الخدمات الاستعلامية التي يريدها[٣].

ويثور تساؤل في هذا الخصوص، هل يعد البنك الإلكتروني العامل عبر شبكة الإنترنت بالمعنى السابق بنكا من الناحية القانونية؟ بمعنى آخر هل يستجمع البنك العامل عبر شبكة الإنترنت المفهوم القانوني للبنك؟

(٤) مدى اعتبار البنك الإلكتروني على شبكة الإنترنت بنكا من الناحية القانونية:

٢٣- يقتضي التعرض لهذا الأمر الوقوف على التعريف القانوني للبنك، وذلك من أجل النظر في مدى دخول البنك العامل على شبكة الإنترنت بالمفهوم السابق تحت هذا التعريف من عدمه.

الملاحظ على موقف التشريعات القانونية في هذا الخصوص أنها أنقسمت إلى

---

(1) **M.Sklira. A.S.pomportsis. M.S. Obaidat**. A framework for the design of bank communications, Computer communication, 2003, p. 1776. available at: www.ComputerScienceWeb.com

(2) **Shaoyi Liaoa and other**; Op. Cit, p. 63.

(3) **Ibid**., p. 67.

اتجاهين:

الاتجاه الأول: عدم وضع تعريف محدد للبنك:

يأتي في مقدمة النظم القانونية التي لم تضع تعريفا محددا لما يقصد بالبنك، النظام القانوني المصري، حيث يخلو من نص محدد يعرف البنك. فالقانون رقم ٢٠ لسنة ١٩٧٥ في شأن البنك المركزي المصري والجهاز المصرفي لم يتضمن تعريفا للبنك، أيضا القانون رقم ٨٨ لسنة ٢٠٠٣ لم يتعرض لهذا الأمر. لكن القانون الأخير تعرض لما يقصد بعمليات البنوك، وعرفها بأنها " كل نشاط يتناول بشكل أساسي أو اعتيادى قبول الودائع والمدخرات، واستثمار تلك الأموال في تقديم التمويل والتسهيلات الائتمانية، والمساهمة في رؤوس أموال الشركات، وكل ما يجرى العرف المصرفي على اعتباره من أعمال البنوك"[١].

هذا وقد استعاض المشرع المصري عن وضع تعريف للبنك، بوضع بعض الشروط[٢] التي يجب أن تتوافر حتى يرخص للمنشأة بمباشرة العمل المصرفي ومن ثم تعد بنكا؛ وهي كما نصت المادة ٢٣ من القانون سالف الذكر:

(١)أن يتخذ البنك أحد الأشكال الآتية:

أ- شركة مساهمة مصرية، جميع أسهمها اسمية.

ب-شخص اعتباري عام يكون من بين أغراضه القيام بأعمال البنوك.

ج- فرعا لبنك أجنبى، يتمتع مركزه الرئيس بجنسية محددة ويخضع لرقابة

---

(١) انظر **د. محي الدين إسماعيل علم الدين**، شرح قانون البنك المركزي والجهاز المصرفي والنقد رقم ٨٨ لسنة ٢٠٠٣، **دار النهضة العربية**، ٢٠٠٤، ص ٥٩.
(٢) انظر تفصيل هذه الشروط لاحقا، ص ٢٤٥.

سلطة نقدية في الدولة التي يقع فيها مركزه الرئيس.

(٢) ألا يقل رأس المال المصدر والمدفوع بالكامل عن خمسمائة مليون جنيه مصري، وألا يقل رأس المال المرخص به لنشاط الفروع الأجنبية في جمهورية مصر العربية عن خمسين مليون دولار أمريكي أو ما يعادلها بالعملات الحرة.

(٣) أن يعتمد محافظ البنك المركزي بعد موافقة مجلس إدارته النظام الأساسي للبنك وعقود الإدارة التي يتم إبرامها مع أي طرف يعهد إليه بالإدارة، ويسرى هذا الحكم على كل تجديد أو تعديل للأنظمة الأساسية أو لعقود الإدارة.

وينضم إلى النظام القانوني المصري في هذا الاتجاه تشريعات الأخرى نأت بنفسها عن وضع تعريف محدد للمقصود بالبنك. لكن الملاحظ على هذه التشريعات أنها صاغت معايير محددة هي بمثابة الحد الأدنى، إذا ما توافرت يمكن القول بأننا بصدد بنك(١). ومن هذه التشريعات قانون البنوك الفرنسي الصادر سنة ١٩٤٠ والمعدل بقانون سنة ١٩٨٤ حيث لم يتضمن تعريفا محددا للبنك، ولكن تضمن مجموعة من الأحكام تشير إلى أن البنك مؤسسة تتلقى الودائع النقدية من الجمهور، وأن هذا ما يميزها عن المؤسسات المالية الأخرى التي تعمل بأموالها الخاصة دون أن تجمع هذه الأموال من الجمهور. أيضا قانون البنوك الإنجليزي الصادر سنة ١٩٨٦ لم يتضمن تعريفا منضبطا للبنك، لكن شراح هذا القانون خلصوا منه بمجموعة من

---

(١) انظر هذه القوانين د.**علي جمال الدين عوض**، عمليات البنوك من الوجهة القانونية، الطبعة الثالثة، دار النهضة العربية، ٢٠٠٠، ص١١،١٢.

الخصائص يرون أن توافرها في مؤسسة ما يجعلها بنكا، وهي:

١- قبول النقود من العملاء كوديعة .

٢- تحصيل الشيكات المستحقة للعملاء.

٣- وفاء الشيكات والأوامر الصادرة من العملاء على حساباتهم .

٤- فتح حسابات جارية .

الاتجاه الثاني- وضع تعريف محدد للبنك:

ولم يظهر لنا من التشريعات التي تبنت هذا الاتجاه إلا القانون التجاري الموحد في الولايات المتحدة الأمريكية (UCC)(١). الذي عرف البنك في المادة الأولى فقرة (٢) بأنه "أي شخص قانوني يحترف تقديم الخدمات المصرفية".

وبصورة عامة يمكن القول برجحان الاتجاه الأول؛ حيث يجدر بالتشريعات القانونية دائما ألا تقحم نفسها في مجال وضع التعريفات خاصة في مجال عمل البنوك؛ لما تتميز به البنوك من تطور دائم في أنشطتها وفي أسلوب تعاملها مع عملائها، الأمر الذي وإن حدث (وضع تعريفات تشريعية في مجال المعاملات المصرفية) قد يحد من حرية الحركة والعمل بالنسبة لهذه البنوك .

لكن في ضوء ما تم الوقوف عليه من اتجاهات التشريعات السابقة، سواء من عرف البنك منها، أم ما اكتفى بوضع معايير أو خصائص كي نكون بصدد بنك، نلاحظ أنها ركزت في سبيل تحديد المقصود بالبنك على نشاط هذه البنك،

---

(1) **Uniform Commercial Code**, 1997, (article 1) general provisions, (part 2) general definitions and principles of interpretation.

وليس على الشكل الذي يظهر فيه ولا على أسلوب تقديمه للخدمة المصرفية وتعامله مع عملائه، بمعنى أنها تبنت معيارا موضوعيا، يربط وجود البنك من الناحية القانونية، بطبيعة الخدمات التي يقدمها، يستوي بعد ذلك أن يكون لهذا البنك كيان مادي متمثل في أبنية ومعدات، أم له كيان إلكتروني متمثل في مجموعة من الأجهزة والبرمجيات، الأمر الذي يمكن معه القول باعتبار البنك الإلكتروني العامل عبر شبكة الإنترنت بنكا من الناحية القانونية؛ فهو يقدم كافة الخدمات والأنشطة المصرفية من تلقى ودائع الأفراد وإعادة إقراضها، وإجراء عمليات الدفع، وتحصيل الشيكات والوفاء بقيمتها وباقي العمليات المصرفية الأخرى وذلك بطريقة إلكترونية.

يضاف إلى ذلك، أن التشريعات التي وضعت شروطا يجب توافرها في المؤسسة التي تقدم الخدمات المصرفية (القانون المصري، والإنجليزي)، أن هذه الشروط لا تتضمن ما يمنع من وجود بنك ينشأ ويؤدى خدماته بطريقة إلكترونية عبر شبكة الإنترنت.

٢٤- نخلص من ذلك بنتيجة محددة، وهي أن النظام القانوني المصري فيما يتعلق بتنظيم نشاط البنوك، ليس فيه ما يعارض إمكانية وجود بنك إلكتروني ينشأ ويؤدى خدماته عبر شبكة الإنترنت، متى استوفى الضوابط والمعايير التي وضعها لممارسة العمل المصرفي. وبناء عليه يعد البنك الإلكتروني العامل عبر شبكة الإنترنت بنكا في ضوء أحكام القانون المصري.

الباب الأول

إنشاء البنك الإلكتروني على شبكة الإنترنت والرقابة عليه

٢٥- يحتل الحديث عن التنظيم القانوني لإنشاء البنك الإلكتروني على شبكة الإنترنت والرقابة عليه أهمية خاصة في هذه الدراسة. فالمفهوم الجديد لإنشاء هذا البنك والرقابة عليه، عكس العديد من القضايا القانونية حديثة العهد في نظام عمل البنوك، وفرض العديد من التحديات، التي باتت في حاجة إلى معالجة قانونية تراعى الطبيعة الخاصة لإنشاء البنك والرقابة عليه في ضوء مختلف العوامل المؤثرة فيه.

فقد أكسبت الطبيعة الإلكترونية للبنك إنشاءه مفهومًا مغايرًا لإنشاء البنك التقليدي، وطرحت في المقابل العديد من التساؤلات حول طبيعة التكوين الفني للبنك وكيفية عمله على شبكة الإنترنت. وطبيعة علاقة البنك بموردي الأجهزة والبرامج من ناحية، وعلاقته بمقدمي الخدمات الإلكترونية من ناحية آخري، وما يتمخض عن هذه العلاقات من التزامات قانونية، وما يترتب على الإخلال بها من مسؤوليات، وذلك في ضوء الطبيعة القانونية الخاصة لنظام عمل البنوك.

أيضا أكسبت البيئة الإلكترونية المفتوحة على العالم بأسره- شبكة الإنترنت- الرقابة على البنك أهمية خاصة؛ مصدرها حجم ونوعية المخاطر الناجمة عن تواجد البنك وممارسته لنشاطه المصرفي عبر الأجهزة الإلكترونية ووسائل الاتصال عن بعد. فعلى الرغم مما تقدمه شبكة الإنترنت للبنك وللمتعاملين معه من مزايا، إلا أنها في ذات الوقت منبع متدفق من المخاطر من شأنه أن يعصف

بوجود البنك، ما لم تتخذ الاحتياطات الرقابية اللازمة لذلك من قبل البنك تحت إشراف جهة الرقابة، والتي تعمل على وضع معايير رقابية تسعى إلى مواجهة هذه المخاطر، وتفرض على البنك الالتزام بها حتى تمنحه الترخيص بالإنشاء، وممارسة العمل المصرفي على شبكة الإنترنت.

لذلك سينتظم الحديث في هذا الباب على فصلين، الأول نعرض من خلاله لإنشاء البنك الإلكتروني على شبكة الإنترنت. والثاني، للرقابة عليه، وذلك على النحو التالي:

الفصل الأول

إنشاء البنك الإلكتروني على شبكة الإنترنت

٢٦- يحظى إنشاء البنك الإلكتروني على شبكة الإنترنت بمفهوم مختلف عن إنشاء البنك التقليدي. وليس مصدر هذا الاختلاف في الأساس العمليات المصرفية التي يؤديها كل بنك عن الآخر، ولكن مصدره البيئة التي ينشأ فيها البنك الإلكتروني، والوسيلة التي يؤدى بها خدماته وهي شبكة الإنترنت. فإذا كان إنشاء البنك التقليدي يتم باختيار قطعة أرض، ومجموعة من مواد البناء المتعارف عليها لإنشاء مبنى البنك، وتزويده بالأثاثات اللازمة، فإن الأمر مختلف تماما عند الحديث عن إنشاء البنك الإلكتروني على شبكة الإنترنت، حيث إن الإنشاء في الحالة الأخيرة يستعيض عن قطعة الأرض ومواد البناء، بمجموعة من الأجهزة الإلكترونية المترابطة فيما بينها بطريقة معينة، والمتصلة بشبكة الإنترنت(١).

(1) **S.K. Leong T. Srikanthan, G.S.Hura**, An internet application for

ومن هنا تظهر الأهمية القصوى للتكنولوجيا ووسائل الاتصالات كأدوات لإنشاء وتشغيل البنك الإلكتروني على شبكة الإنترنت[١]. لكن هذه الأهمية لا تعنينا لذاتها، ولكن لانعكاساتها القانونية، والتي تمثلت في خلق شبكة من العلاقات القانونية الحديثة في نظام عمل البنوك، أهم ما يميزها أنها متشابكة ومترابطة، وذات تأثيرًا مباشر في النشاط المصرفي للبنك[٢].

والأمر على هذا النحو يحتاج إلى ضرورة التعرض ـ ولو سريعًا ـ لطبيعة التكوين الفني للبنك الإلكتروني على شبكة الإنترنت؛ وذلك لتقريب الرؤية قدر الإمكان حول طريقة عمل البنك وطبيعة الوظائف والأداءات المختلفة لمن يقدمون الأدوات والخدمات الإلكترونية له، حتى يأتي التنظيم القانوني ملائما ومتناسبا لواقع وطبيعة هذه الوظائف والأداءات.

وبناء عليه، سوف ينتظم الحديث عن إنشاء البنك الإلكتروني على شبكة الإنترنت على النحو التالي: التصميم الفني لشبكة البنك الإلكتروني والعقود اللازمة لذلك (مبحث أول) عقود الخدمات الإلكترونية اللازمة لتشغيل البنك على شبكة الإنترنت (مبحث ثاني).

---

on-line banking, computer communication, Elsevier, 1997, p. 1535.

(١) د. **سعيد الحامز**، العمليات المصرفية الإلكترونية والإطار الإشرافي، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ هـ ١٠-١٢ مايو ٢٠٠٣ دبي، ص ٢٣٣٨.

(2) **John Carlson, Karen Furst, William W.Lang, Daniel E.Nolle**, internet banking: **Market Developments and Regulatory Issues**, Society of government economists conference, May 2001, p. 21. available at: www.occ.treas.gov/netbank/sgec2000.pdf.

المبحث الأول

التصميم الفني للبنك الإلكتروني

والعقود اللازمة لذلك

٢٧- يلاحظ من خلال تدقيق النظر في التصميم الفني للبنك الإلكتروني العامل على شبكة الإنترنت، أنه عبارة عن شبكة إلكترونية[١] داخلية، تضم مجموعة من الأجهزة والمعدات (حاسبات شخصية، محطات عمل، حاسبات متوسطة،

---

(١) وتعرف الشبكة الالكترونية **Networks** بأنها عبارة عن اتصال بين اثنين من الحاسبات أو أكثر (سلكيا أكان أو لا سلكيا) بغرض اتصال الأشخاص وتبادل المعلومات والسماح بالمشاركة في موارد الحاسب. انظر في ذلك د. **نشأت الخميسي**، برامج التعامل مع الويب، التجارة الإلكترونية، أكاديمية السادات للعلوم الإدارية – سلسلة إصدارات البحوث الإدارية، الإصدار (٣)، ٢٠٠١ ص٨٣.

– وتنقسم شبكات الحاسبات من حيث التغطية الجغرافية إلى ثلاثة انواع * **شبكات الحاسبات المحلية** (Local Area Network)، وتتميز بكونها محدودة المسافات (لا تتجاوز بعض الكيلومترات) بين الحاسبات التي تربطها أو كونها مملوكة لمؤسسة ما، وتتميز كذلك بسرعتها الفائقة لنقل البيانات والتي تتراوح بين ١. إلى ١٠.. أو ١٠... ميجا بت في الثانية * **شبكات الحاسبات الإقليمية** (MetrOpolitan Area Network)، وتستخدم الشبكات الإقليمية في مساحات جغرافية متوسطة نسبيا تصل إلى عدة كيلومترات، وتستعمل في ربط حاسبات موجودة في نفس المدينة أو مجموعة قريبة من المدن وتتراوح السرعة في هذه الشبكة بين ٤ إلى ١... ميجا بت في الثانية * **شبكات الحاسبات الواسعة** (Wide Area Network)، وهذه الشبكة عبارة عن مجموعة من الشبكات الالكترونية المرتبطة على نطاق واسع، لتغطى منطقة جغرافية واسعة تمتد لآلاف الكيلومترات، وسرعة هذه الشبكة ضعيفة بالمقارنة بالشبكات المحلية والإقليمية، حيث تعتمد على شبكة الهاتف ومجموعة كبيرة من أجهزة المودم. راجع العنوان الإلكتروني التالي:

http://www.awrag.com/fm//archive/index.php/t-5868.html

حاسبات كبيرة) القادرة على التعامل مع التطبيقات المالية، بالإضافة إلى بعض الأجهزة الملحقة (جهاز تقوية، مجمعات توصيل، جسر أو مسار ربط)، والمترابطة فيما بينها بمجموعة من وسائل الربط المختلفة (وحدات ربط Network Cards، كوابل محورية، أسلاك مبرومة وألياف ضوئية)، والتي تعمل على ربط هذه الأجهزة والمعدات على نحو يجعل مجموع هذه الأجهزة والمعدات وحدة واحدة مترابطة يطلق عليها " شبكة البنك الإلكترونى"(١).

والأمر على هذا النحو يدفعنا لإلقاء نظرة على التكوين الفني لشبكة البنك الإلكتروني، وذلك للتعرف على مكوناتها الخاصة (مطلب أول)، وتحديد العقود اللازمة لتوفير هذه المكونات في ضوء طبيعة كل مكون، وطبيعة عمله في شبكة البنك الإلكتروني (مطلب ثاني).

المطلب الأول

التصميم الفني لشبكة البنك الإلكترونى

أولا- طريقة تصميم شبكة البنك الإلكترونى:

٢٨- يمكن أن تظهر شبكة البنك الإلكتروني بالمفهوم السابق من حيث طريقة

(1) **S.K. Leong T. Srikanthan, G.S.Hura**, An internet application for on-line banking, Computer Communication, Elsevier, 1997, p. 1535;

- http://www.awrag.com/fm//archive/index.php/t-5868.html

التصميم في أحد شكلين، على النحو التالي:

الشكل الأول: تصميم شبكة البنك الإلكتروني بطريقة (المزود- العميل Server – Client)

تصمم شبكة البنك الإلكتروني في هذا الشكل على أساس وجود حاسب مركزي يسمى (Server)، يحتوى على مساحة تخزين كبيرة، ومعالج قوى (CPU)، ويتميز بسرعة فائقة، ويرتبط هذا الحاسب بمجموعة من الحواسيب الصغيرة المنتشرة في مواقع مختلفة على شبكة البنك(والتي تسمى العميل Client)، حيث يعمل الحاسب المركزي على تزويد كافة الحواسيب والأجهزة العاملة على شبكة البنك بالبرامج والبيانات اللازمة لتشغيل البنك، كما يعمل على تنظيم مجريات العمل المصرفي على نطاق شبكة البنك؛ وذلك من خلال توزيع مهام العمل المختلفة على الأجهزة كل بحسب وظيفته(١).

ويمكن في هذا التصميم من الشبكات أن تتم الاستعانة بأكثر من حاسب مركزي، وذلك بحسب ما يتلاءم مع طبيعة، وحجم العمليات المصرفية التي يقوم بها البنك. ويطلق على هذا النوع من الشبكات أيضا الشبكة القائمة على مزود (Server Based Network)(٢).

---

(1) **Jeffrey F.Rayport**, **Bernard j.jaworski**, Introduction to e-Commerce, The McGraw-hill companies, International edition, 2003, p. 341; **Ferguson, Renee Boucher**, Financial system integration tools on way, Vol. 19, Issue 13. Academic Search Complete, 49.

(٢) **د. محمد سعيد إسماعيل**، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق – جامعة عين شمس، ١٤٤٦ هـ – ٢٠٠٥ م، ص ٢٨؛

الشكل الثاني: تصميم شبكة البنك الإلكتروني بطريقة (النظير- للنظير) (Peer to peer)

تصمم شبكة البنك الإلكتروني في هذا الشكل على أساس وجود مجموعة من الحاسبات المتناظرة في الإمكانيات والمترابطة فيما بينها، حيث يتميز هذا التصميم بعدم وجود حاسب مركزي يعمل كمزود لباقي الأجهزة، بل يقوم كل جهاز مرتبط بالشبكة بدور المزود والعميل في ذات الوقت(١).

٢٩- وأيا ما كان الشكل الذي ستصمم شبكة البنك الإلكتروني فيه، فأن هناك قاسما مشتركا من الخصائص يجب أن تتمتع به هذه الشبكة، وذلك مراعاة لمتطلبات تقديم الخدمات المصرفية. ومن أهمها(٢):

- إتاحة الاستفادة من المكونات المختلفة(أجهزة ومعدات وبرامج) على شبكة البنك، وذلك من خلال ربطها،على نحو يمكن فيه لكل مكون أن يستفيد من خدمات باقي المكونات، سواء كانت مكونات مادية (الطبعات، الماسح الضوئيScanner)، أم معنوية (قواعد البيانات، أو صفحات

Client-server, Wikipedia; The free encyelopedia, available at: http://en. wikipedia.org/wiki/Client-server

(١) د. محمد سعيد إسماعيل، المرجع السابق، ص ٢٨؛

Peer-to-peer, From Wikipedia, The free encyelopedia, available at; http://en. wikipedia. org/wiki/Peer-to-peer

(٢) راجع هذه الخصائص على العنوان الإلكتروني التالي:

http://www.awrag.com/fm//archive/index.php/t-5868.html; **Jean Pionnier**, Sécurité informatique (un nouvea souci de l'inspection bancaire), Theme de la Journee organisee le mercredi , No3-Mars 1985,p 156.

الويب الخاصة بموقع البنك)، وذلك بغرض جعل الشبكة كلها وحدة واحدة لخدمة النشاط المصرفى. والقول بإتاحة الاستفادة من المكونات المختلفة للشبكة لا يخل بحق البنك بحظر التعامل مع بعض الموارد التي تحتوى على بيانات ذات طبيعة خاصة- مثل الأجهزة التي تحتوى على البيانات التي تعد من الأسرار المصرفية- حيث يقرر البنك حظر التعامل معها إلا من قبل أشخاص معينين.

- قدرة أجهزة الشبكة على تنفيذ المهام المطلوبة بسرعة فائقة، سواء كانت هذه المهام تتم بين العاملين على شبكة البنك (تطبيقات رياضية، عمليات تبادل للبيانات)، أم كانت تتم استجابة لطلبات العملاء (العمليات المصرفية) الذين يتعاملون مع هذه الأجهزة عبر موقع البنك على شبكة الإنترنت. ويبرر ذلك أن شبكة البنك تؤدى خدمات فورية تفاعلية (وليس مجرد خدمات إعلانية بسيطة) على شبكة الإنترنت، بما لا يقبل معه التراخي أو التباطؤ في تنفيذ المهام.

- الاستعانة بمجموعة من الأجهزة البديلة، بحيث تعمل على تشغيل البنك في حالة وجود أي عطل أو خلل فجائى في نظام عمل الشبكة. ويجب أن تكون هذه الأجهزة في حالة تأهب دائمة، ولديها قدرة التغلب على الصعاب الفجائية، بحيث تقدم حلا سريعا وجاهزا في حالات الطوارئ. ويمثل هذا الأمر أهمية بالغة في نظام عمل البنك؛ وذلك لارتباط انتظام تقديم الخدمة المصرفية بالسمعة التجارية للبنك.

- الاستعانة بمجموعة من الفنيين المتخصصين في شؤون الحاسبات والشبكات ذات التطبيقات المالية، وذلك للقيام بإجراءات الفحص الدوري

لكل الأجهزة العاملة على الشبكة لاكتشاف أي خلل أو عطل، والقيام بأعمال الصيانة اللازمة لمواجهة هذه الأمور.

ثانيا- مكونات شبكة البنك الإلكتروني:

٣٠- يتضح من خلال العرض السابق للتصميم الذي يمكن أن تظهر عليه شبكة البنك الإلكتروني، أنه يتكون من مجموعة من الأدوات التقنية، ومجموعة من وسائل الربط، وذلك على النحو التفصيل التالي:

١)- مجموعة من الأدوات التقنية:

تتكون شبكة البنك الإلكتروني من مجموعة من الأدوات التقنية (أجهزة وبرامج)، القادرة على التعامل مع التطبيقات المالية، والتي تتناسب مع حجم وطبيعة النشاط المصرفي الذي سيؤديه البنك على شبكة الإنترنت [١]. ومن أهم هذه الأدوات [٢]:

أ- **حاسب آلي كبير**، وهو عبارة عن جهاز كمبيوتر مركزي يعمل كخادم (Server)[٣]، يتلقى عبر شبكة الإنترنت طلبات العملاء الخاصة بالخدمات المصرفية، ثم يتعرف على طبيعة هذه الطلبات، ويوجهها بحسب طبيعة

---

(1) **M. Sklira. A. S.pomportsis. M.S. Obaidat**; Op. Cit, p. 1776; S.K **Leong, T. Srikanthan, G.S. Hura,** An internet application for on line banking, Computer Communication (Elsevier), p 1537

(2) **Joris Claessens - Valentin Dem- Danny De Cock-Bart Preneel- Joos Vandewalle**: Op. Cit., p. 256.

(3) **Julian JB Hickey – Robin Mathew-ChristOpher**; E-commerce: law, business and tax planning, Jordan's, 2000, p 7; E- Banking, Federal Financial Institutions Examination Council; Op. Cit., p 4.

الخدمة المطلوبة إلى الأجهزة المختصة على شبكة البنك[١]. وغالبا مـا يـتم الاستعانة ببروتوكول[٢] (SNA)[٣] في تنظيم عملية اتصال هذا الحاسب بباقي الأجهزة على الشبكة.

ب- **خادم لموقع البنك على شبكة الإنترنت**[٤]، وهو عبارة عن جهاز كمبيوتر متصل بشبكة الإنترنت، يعمل على عرض وتخزين صفحات الويب (Web) الخاصة بالموقع الإلكتروني للبنك على شبكة الإنترنت، من وإلى مستعرض الصفحات (Web browsers)[٥]. ويربط هذا الخادم بشبكة البنك الداخلية ما يسمى تطبيقات الخادم (Application Server)، وهي عبارة عن مجموعة

---

(1) **U.S. Consumers and Electronic Banking,** 1995-2003, available at:
www.federalreserve.gov/pubs/ bulletin/2..4/winter.4_ca.pdf;
Jeffrey F. Rayport, Bernard J. Jaworski, Op. Cit., p 341.

(٢) وكلمة بروتوكول protocol "تعنى مجموعة القواعد التي تقدم توصيفا فنيـا لكيفيـة تنفيذ شيء ما " انظر في ذلك د. **نشأت الخميسي**، مرجع سـابق، ص ٨٤. وعرفـه البعض أيضا بأنه عبارة عن "مجموعة القواعد الإرشادية والمبادئ المتحكمة في عمل شبكة ما، وقواعد البيانات والإرشادات الإلكترونية على هذه الـشبكة، وكيفيـة بـث المعلومات، والدخول إلى هذه الشبكة، ومعالجة التطبيقات الخاصة بها" انظر **د. طارق عبد العال حماد**، التجارة الإلكترونية، الدار الجامعية، ٢٠٠٣، ص٤، ٨.

(٣) وهـو برتوكـول خـاص بهندسـة وبنـاء الـشبكات **Systems Network (Architecture)**.

(4) **E-Banking,** Federal financial institutions examination council; Op. Cit., p. 4.

(5) **S.K Leong, T. Srikanthan, G.S. Hura** Op. Cit, p. 1539, **Michael chissick, Alistair Kelman**, Electronic commerce law and practice, Third edition, Sweet & Maxwell, 2002, P xliii.

من البرمجيات تعمل كحلقة وصل بين خادم الموقع والشبكة الداخلية للبنك(١).
ويعتمد خادم موقع البنك الإلكتروني في عملــه علــى بروتوكــول يــسمى (TCPL/IP)(٢).

ج- **أنظمة إنذار إلكترونية (Alarm Systems)**، وهذه الأنظمــة تلحــق بالموقع الالكتروني للبنك على شبكة الإنترنت، وتعمل على مراقبة هذا الموقع من خلال إعطاء إشارات (صوتية أو ضوئية) في حالة تواجد أي بيانــات أو برامج ذات طبيعة غريبة على هذا الموقــع؛ كبيانــات أو بــرامج محملــة بفيروسات، أو حدوث دخول على موقع البنك دون المرور بإجراءات التوثيق المقررة لذلك. وتحتل أنظمة الإنذار بهذا المعنى أهمية كبرى في نظام عمــل البنك، وذلك بالنظر إلى أهمية الاعتبارات التي تقف وراء تأمين البنك، والتي يأتي في مقدمتها زيادة احتمالية تعرض البنك للانتهاكات والاختراقات علــى شبكة الإنترنت.

د- **أنظمة للتحكم المالي (Financial Controller Systems)**: وهــي عبارة عن مجموعة من أجهزة الاتــصالات الثنائيــة المتزامنــة (Binary Synchronous communications)، والتي يلحق بهــا مجموعــة مــن البرمجيات الخاصة بالتعاملات المالية(٣). وتعمل هذه الأجهزة علــى دعــم

---

(١) د. **طارق عبد العال حماد**، مرجع سابق، ص ٧٧١.

(٢) وهذا اختــصار لبروتوكــول **Transmission control protocol/Internet protocol**، وهو بروتوكول يعمل على تقسيم المعلومات القادمة إلى البنك الإلكتروني إلى حزم Packets، وذلك تمهيدا لتوزيعها على الأجهزة العاملة على الشبكة؛ انظر:
Michael chissick, Alistair Kelman, Op. Cit, p. xliii.

(3)**Julian JB Hickey – Robin Mathew-ChristOpher**; Op. Cit, p. 16

مرور البيانات المالية في هيكل شبكة البنك، وتنظيم حركة هذه البيانات على أطراف الشبكة، ويربط بين هذه الأدوات مجموعة من خطوط الربط، والتي تسمى (Synchronous Data Link). فمثلا تقوم هذه الخطوط بالربط بين جهاز السيطرة على التطبيقات المالية المركزية، والأجهزة الخاصة بالتعاملات المصرفية، مثل ماكينات سحب النقود (ATM)(١).

ويجب ملاحظة أن ما سبق ذكره هو مجرد توضيح للمكونات الأساسية اللازمة لتكوين شبكة البنك الإلكتروني، والتي يلحق بها مجموعة من المكونات الثانوية مثل؛ الطابعات والماسحات الضوئية والفاكسات بحسب الحاجة (٢). ويجب على البنك عند قيامه بإبرام العقود اللازمة لتوريد هذه الأجهزة، أن يراعى التعاقد على الكمية التي يراها مناسبة لحجم ونوعية تعاملاته، وطبيعة العملاء الذين يتعامل معهم.

٢)- مجموعة من وسائل الربط:

تحتاج الأدوات التقنية سالفة الذكر إلى مجموعة من وسائل الربط لتكوين شبكة متكاملة ومترابطة تصلح لعمل البنك الإلكتروني. وتقوم هذه الوسائل بدور هام؛ حيث تدعم مرور البيانات بين الأجهزة العاملة على شبكة البنك. كما أن حفظ هذه البيانات ضد محاولات التجسس والاطلاع غير المشروع مرهون بجودة هذه الوسائل (٣). ومن أهم وسائل الربط؛ بروتوكول لتنظيم حركة البيانات،

---

(1) **M.Sklira. A. S. pomportsis. M.S. Obaida**; Op. Cit., p. 1775.

(٢) انظر العنوان التالي:
http://www.syriacomp.com/ic/part1.htm

(٣) انظر العنوان التالي:

ووسائط للنقل (كابلات توصيل)، وكروت اتصال، وذلك على التفصيل التالي:

أ- بروتوكول لتنظيم حركة البيانات:

توجد العديد من البروتوكولات التي تستخدم في تنظيم حركة البيانات في الشبكات الإلكترونية بصورة عامة. ويحدد نوع البروتوكول المطلوب في ضوء طبيعة عمل الشبكة وأغراضها(١). ويعد بروتوكول(Ethernet) (٢) وبروتوكول (Token Ring) (٣)من أهم البروتوكولات المستخدمة في شبكة البنك الإلكتروني، خاصة بروتوكول "Ethernet"(٤). وتتلخص طريقة عمل هذا

---

http://www.arablaw.org/Download/E-Banking.doc

(١) يتوقف تحديد نوع البروتوكولات المراد استخدامها على نوع الشبكات والبيانات والمعلومات المتبادلة. فهناك نوع من البروتوكولات المعروفة باسم TCP/IP(Transmission Control Protocol/Internet Protocol) وهو يعد من أشهر البروتوكولات المستخدمة في شبكة الانترنت، حيث يضم هذا البروتوكول مجموعة من القواعد التي تستخدم لإقامة وإنهاء الاتصالات، وكذلك لتحديد مسار البيانات الصغيرة packets. وهناك نوع آخر من البروتوكولات يستخدم لنقل الملفات، ويسمى (File Transfer Protocol) **FTP** كما يوجد بروتوكول لنقل النصوص المتشعبة والمعلومات المتعددة الوسائط ويسمى http (Hyper Text Transfer)؛ انظر العنوان التالي: http://www.awrage.com/fm//archive/index.php/t-5868.html؛ إبراهيم المنجي، عقد نقل التكنولوجية، منشأة المعارف، الطبعة الأولى، ٢٠٠٢، ص ٢٨٣.

(2) **Adel M. Aladwani,** Online banking: A field study of drivers, International journal of information management, 2001, p 214 ;**Carl Pacini and others,** At the interface of the electronic frontier and the law: The international legal environment for systems Reliability assurance services, Journal of international accounting, Auditing & Taxation- 9 (2) , 2000, p. 188.

(3) **M.sklira – A.s. spomportsis – M.s. Obaidat**; Op. Cit., P. 1777.

(4) **IBM,** Banks form financial services net, Electronic news, Vol. 42,

البروتوكول في قيامه بتجزئة البيانات التي يتضمنها الملف المراد إرساله إلى أجزاء رقمية صغيرة تسمى" packets "[١]؛ حيث يحتوى كل جزء على عنوان الكمبيوتر المرسل إليه. كما يعمل البروتوكول بعد ذلك على نقل هذه الأجزاء في صورة دفعات متتالية[٢]، ولا يسمح إلا لجزء واحد فقط، في الوقت الواحد بالدخول لشبكة البنك الإلكتروني، وذلك بسبب السرعة الكبيرة التي تتم بها تلك العملية، حيث إن وصول الجزء يكون في جزء متناه في الصغر من الثاني، بحيث يسمح للجزء الثاني بالوصول للشبكة بشكل فوري ومتتال[٣].

Issue 2134, Database: Academic Search Complete, p. 50.

(١) ويمكن أن تحتوى هذه الحزم على أي نوع من المعلومات الرقمية؛ كملفات الكتابة والصور والفيديو.

(٢) حيث إن كل كمبيوتر يعمل في منظومة شبكة البنك الإلكتروني يجب أن يثبت به لوحة الكترونية خاصة "بطاقة اتصال"، حيث تعمل على وصل الكمبيوتر بخطوط الاتصالات في شبكة البنك الإلكتروني وتجعله متفاعلا معها، وتسمى هذه البطاقة Network Interface Card. (NIC) ويوجد بداخل كل بطاقة رمز مميز خاص بها، وهذا الرمز يوجد على رقاقة الكترونية صغيرة " Micro chip ". ويكون هذا الرمز بمثابة عنوان الكمبيوتر الذي تكون هذه اللوحة الإلكترونية مثبتة به، ويستعمل بروتوكول الايثرنت هذا العنوان ليتعرف على كل واحد من أجهزة الكمبيوتر الموجودة على الشبكة، وهذا يسمح لكل حزمة الكترونية يتم إرسالها من جهاز إلى آخر بأن تحتوى على العنوان المرسلة منه وأن تصل فقط للعنوان المرسلة إليه. ويلاحظ أن كل كمبيوتر متصل بشبكة البنك الإلكتروني يقوم بالتعرف على جميع الحزم المارة خلال الشبكة، ولكنه لا يستطيع أن يستجيب إلا إلى الرزم التي تحمل عنوانه. وعندما يقوم كمبيوتر ما بوضع الرزم على شبكة البنك الإلكتروني لإرسالها إلى جهاز آخر متصل بالشبكة لتنفيذ عملية معينة، فإنها تبث إلى جميع أجهزة الكمبيوتر الأخرى على الشبكة، ولكن الكمبيوتر الذي سيستجيب لها ويدعى بأن تلك الرزم تخصه هو الكمبيوتر الذي يحمل عنوان المرسل إليه الذي تحمله تلك الحزم ومن ثم يسمح لهذا الكمبيوتر بالحصول على المعلومات التي تتضمنها تلك الرزم. راجع العنوان الإلكتروني التالي: http://www.syriacomp.com/ic/part1..htm

(٣) هذا بالإضافة إلى أن بروتوكول الايثرنت يتضمن أسلوبا خاصا يتفادى إرسال حزم

ب- وسائط النقل (كابلات توصيل):

تقوم وسائط النقل بعملية نقل البيانات داخل شبكة البنك الإلكتروني، وهي عبارة عن مجموعة من الأسلاك والكابلات[1]. وتوجد عدة أنواع من هذه الأسلاك، ويحدد نوع السلك المطلوب في ضوء مجموعة من العوامل، أهمها: سرعة النقل (Transmission Speed)، وأقصى طول للسلك (Maximum Length)، ومدى مقاومة السلك للتداخل (Shielding Against Interference)[2]. وتوجد ثلاثة أنواع من الأسلاك التي تستخدم في شبكة البنك الإلكتروني، وذلك على التفصيل التالي:

- **الأسلاك المفتولة (المبرومة) Twisted Pair**[3]:

وتتميز هذه الأسلاك بسهولة ربطها مع أي نوع آخر من الأسلاك[1]. وعلى

المعلومات من جهازي كمبيوتر في الوقت ذاته. فإذا حاول (NIC) بث حزمة داخل شبكة البنك الإلكتروني، فانه يقوم أولا بفحص الشبكة؛ ليرى إذا ما كانت هناك حزم يتم إرسالها واستقبالها من الأجهزة الأخرى على شبكة البنك الإلكتروني. فإذا كانت هناك حزم أخرى، فإنه يكون مجبرا على الانتظار (مدة أجزاء متناهية الصغر من الثانية) قبل أن يبدأ البث. ويبقى كذلك حتى يجد البروتوكول فراغا يمكن استخدامه في عملية الإرسال. انظر المرجع (سابقا) الموضع ذاته.

(١) انظر العنوان التالي:
http://www.marmarita.com/ub/archive/index.php/t-1.76.html

(٢)انظر العنوان التالي: http://m.dy.net/vb/archive/index.php/t-1584.html

(٣) وهي عبارة عن زوج سلكي نحاسي مكون بطريقة غزلية على شكل ضفيرة. والالتفاف بين هذه الأسلاك على هذا النحو الهدف منه تقليل التداخل الإلكتروني (Electronic Interference). وكانت هذه الكابلات تستخدم في شبكات التليفونات ولكن تستخدم حاليا في الشبكات الرقمية كوسيط للربط. راجع العنوان الإلكتروني التالي:

http://m.dy.net/vb/archive/index.php/t1584..html

الرغم من بطء حركة أنتقال البيانات في هذا النوع من الأسلاك، لكن يمكن تفادى ذلك من خلال تحديث كروت الشبكات بمستوى تكنولوجي عال، على نحو يجعلها تسمح بسرعة عالية لنقل البيانات. وقد أدى هذا إلى أنتشار هذا النوع من الأسلاك (٢).

- **الأسلاك المحورية Coaxial Cable(٣):**

ويتميز هذا النوع من الأسلاك بأنه شائع الاستخدام؛ بسبب قلة كلفته وخفة وزنه وسهولة تركيبه، ويتميز أيضا بالدعم المعدني الذي يمتص الكهرباء الضائعة مما يؤدى إلى تقليل الضجيج (٤).

- **أسلاك الألياف الضوئية Optical Fiber(٥):**

وتتميز هذه الأسلاك بأنها تنقل الإشارات الكهربائية على شكل نبضات ضوئية، ولا تتأثر بالتداخلات الكهرومغناطيسية أو الراديوية. كما تتميز أيضا

---

(١) حيث يمكن ربط شبكة معتمدة على أسلاك(Twisted Pair) مع شبكة أخرى معتمدة على الأسلاك المحورية (Coaxial Cable)، وذلك لتكوين ربط بين الشبكات (Interconnected).

(٢) انظر المرجع (السابق) الموضع ذاته.

(٣) وهي عبارة عن لب معدني core يقوم بنقل الإشارات الكهربائية، يحيط به عازل كهربائي وطبقة معدنية تحيط بالعزل، وأخيرا غطاء خارجي مصنوع من مادة غير موصلة كالبلاستيك أو المطاط. راجع العنوان الإلكتروني التالي:

http://www.marmarita.com/ub/archive/index.php/t-1.76.html

(٤) انظر المرجع (السابق) الموضع ذاته.

(٥) وهذه الأسلاك عبارة عن أنبوبة دقيقة جدا مصنوعة من الزجاج، يمر فيها الضوء الذي يحمل البيانات من الجهة المصدرة للبيانات إلى جهة الوصول. هذه الانبوبة محاطة بعاكس وفي نهايتها غطاء حماية. راجع العنوان الإلكتروني التالي:

http://m.dy.net/vb/archive/index.php/t-1584..html

بأنها من أكثر الطرق المأمونة لنقل البيانات، وذلك لصعوبة التجسس عليها، كما أنها تناسب السرعات العالية جدا نظرا لنقاء الإشارة (١).

جـ - بطاقة الاتصال بالشبكة (NIC) Network Interface Card:

تعد بطاقة الاتصال من أهم وسائل الربط بالشبكة، وهي عبارة عن لوحة إلكترونية تثبت داخل الكمبيوتر العامل في شبكة البنك الإلكتروني، وتمكنه من التواصل مع أجهزة الكمبيوتر الأخرى الموجودة على شبكة البنك الإلكتروني. ويطلق على هذه اللوحة "أداة التهيئة والربط مع الشبكة". وتعمل هذه اللوحة في اتجاهين: الأول، داخل الكمبيوتر المثبتة به؛ حيث تعمل على تحريك البيانات من ذاكرة الحفظ إلى الذاكرة العشوائية (RAM) والثاني، خارج الكمبيوتر المثبتة به؛ حيث تتحكم في حركة البيانات من نظام توصيلات شبكة البنك الإلكتروني إلى الجهاز المثبت به (٢).

ومن أهم الوظائف التي تقوم بها بطاقة الاتصال في شبكة البنك ما يلي :

١- تجهيز البيانات القادمة من الكمبيوتر المثبتة به لإرسالها لشبكة البنك الإلكتروني.

٢- التحكم في تدفق البيانات بين الكمبيوتر وبين شبكة البنك الإلكتروني.

---

(١) انظر العنوان التالي:

http://www.marmarita.com/ub/archive/index.php/t-1.76.html

(٢) انظر العنوان التالي:

http://www.syriacomp.com/ic/part1..htm

٣- استقبال البيانات القادمة من شبكة البنك وتحويلها إلى بيانات [١]منطقية.

والواقع أن هناك أنواعا مختلفة من بطاقات الاتصال (NIC)، ولكن هذه البطاقات جميعها تقوم بذات الوظائف السابق ذكرها، والتي تتلخص في كونها أداة تهيئة وربط بين جهاز الكمبيوتر وشبكة البنك الإلكتروني. وعادة ما يتم الاختيار بين هذه البطاقات في ضوء أمرين:

الأول: نوع أسلاك التوصيل؛ حيث إن هناك العديد من أنواع الأسلاك التي يمكن استخدامها لربط شبكة البنك (المبرومة والمحوري والألياف الضوئية)، لذا عند اختيار البطاقة يجب معرفة نوع السلك المستخدم في التوصيل.

الثاني: نوع اللوحة الأم في الكمبيوتر. فيمكن لهذه اللوحة أن تحدد نوع بطاقة الاتصال بالشبكة؛ حيث إنها تحتوى على المعالج المركزي، وهذا المعالج هو الذي يتفاهم مع المكونات الداخلية للكمبيوتر من خلال اتصاله معها، ويتفاهم أيضا مع المكونات الخارجية، والتي من ضمنها بطاقة الاتصال، وذلك عن طريق توصيلات ناقلة للبيانات تصل إلى مداخل خاصة يتم تثبيت البطاقة بها [٢].

---

(١) والبايت هو وحدة شائعة الاستخدام لقياس سعة التخزين في الحاسوب بغض النظر عن نوع المعلومات المخزنة أو وسيلة التخزين يستطيع الكمبيوتر فهمها، ويتكون البايت من وحدات أصغر تسمى البت، وكل بت عبارة عن خانة واحدة من رقم ثنائي له احتمالان فقط إما أن يكون البت صفرًا أو واحدًا. انظر العنوان التالي:
http://ar.wikipedia.org/wiki/%D8%A8%D8%A7%Dg%8A%D8%AA

(٢) انظر العنوان التالي:
http://www.syriacomp.com/ic/part1..htm

المطلب الثاني

العقود اللازمة للحصول على مكونات شبكة البنك الالكتروني

٣١- تختلف طبيعة المكونات المادية (الحواسب الآلية/ وسائل التوصيل) عن المكونات المعنوية (البرامج والبروتوكولات)(١)، اختلافا ذا تأثيرًا على التنظيم القانوني الحاكم لعلاقة البنك الإلكتروني بموردي هذه المكونات. ويقتضى الأمر على هذا النحو أن نعرض أولا للعقود اللازمة للحصول على المكونات المادية، وثانيا للعقود اللازمة للحصول على المكونات المعنوية، وذلك على التفصيل التالي:

(١) فالحاسب الآلي يعرف بأنه عبارة عن مجموعة أجهزة متكاملة مع بعضها بهدف تشغيل مجموعة من البيانات المدخلة بموجب برنامج مثبت للوصول إلى النتائج المطلوبة. ويقوم برنامج الحاسب الآلي بقبول البيانات وتخزينها ومعالجتها من خلال البرامج الموجودة داخل الجهاز بهدف الوصول إلى النتائج المطلوبة، ومعالجة المعطيات المخزونة في الذاكرة الرئيسة في صيغة معلومات تحت إشراف برنامج مخزون. وقد عرف قانون حقوق تأليف برامج الكمبيوتر الأمريكي الصادر عام ١٩٧٦ والمعدل في ١٩٨٠ هذا البرنامج بأنه عبارة عن (مجموعة البياناتِ أو الأوامر التي تستخدم بشكل مباشر أو غير مباشر في الحاسوبِ للوصول إلى نتيجة محددة). انظر في ذلك د. **خالد مصطفى فهمي**، الحماية القانونية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، ٢٠٠٥، ص٧؛ د. **مصطفى محمد عرجاوى**، الحماية المدنية لبرامج الكمبيوتر في القوانين الوضعية، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون (جامعة الإمارات العربية المتحدة)، ٢٠٠٠، ص٧؛
Roger Gerleroy Miler – Gaylord A. Jentz; Op. Cit, p. 116.

أولا- العقود اللازمة للحصول على المكونات المادية لشبكة البنك:

١)- عقد بيع الأدوات التقنية:

٣٢- يقصد بالمكونات المادية اللازمة لتصميم شبكة البنك، مجموعة الأجهزة الإلكترونية (الحواسيب، أجهزة الإنذار)، وأدوات التوصيل (أسلاك، كروت اتصال) التي تلزم لبناء شبكة البنك واتصاله بشبكة الإنترنت. ويلجأ البنك الإلكتروني في سبيل حصوله على هذه الأدوات إلى شرائها من الأفراد أو الشركات التي تقوم ببيعها، وذلك مقابل التزام البنك الإلكتروني بدفع ثمنها تحقيقا للاتفاق المبرم في العقد(١)، ومن ثم فأننا بصدد عقد بيع يخضع في انعقاده وتنفيذه لقواعد عقد البيع (القانون التجاري والمدني).

وعقد البيع كما هو معلوم ينطوي على العديد من الالتزامات التي تقع على عاتق البائع، والتي لا يتسع المجال لعرضها، وخاصة أن الحديث عنها لا يضيف جديدًا في علاقة البنك ببائع الأدوات التقنية. لكن ما يدعو لتسليط الضوء عليه هو الالتزام بالتسليم؛ وذلك بالنظر إلى الطبيعة الفنية لمحل العقد (الأجهزة الإلكترونية)، والغرض من التعاقد (تصميم شبكة إلكترونية للبنك الإلكتروني)، الأمر الذي يجعل هذا الالتزام ذا أهمية بالغة بالنسبة للبنك. والالتزام بالإعلام، وذلك على التفصيل التالي:

(أ) التزام بائع الأدوات التقنية بالتسليم:

٣٣- يعرف الالتزام بالتسيلم بأنه عبارة عن تعهد البائع بأن يضع الشيء المبيع

---

(1) **Chris Reed**, Internet law, Cambridge university press, Second edition, 2004, P 307.

تحت تصرف المشترى.

ويجد هذا الالتزام أساسا تشريعيا له، حيث تنص المادة ٢٠٦ من القانون المدني المصري، على " الالتزام بنقل حق عيني يتضمن الالتزام بتسليم الشيء والمحافظة عليه حتى التسليم". كما نصت المادة ٤٥٣ من ذات القانون على " التسليم هو وضع المبيع تحت تصرف المشترى بحيث يتمكن من حيازته والانتفاع به دون عائق ولو لم يستول عليه ماديا مادام البائع قد أعلمه بذلك".

ويكتسب التزام بائع الأدوات التقنية بالتسليم في مواجهة البنك الإلكتروني مفهومًا خاصًا؛ فالتسليم هنا ليس عملاً ماديا، يتم بمجرد وضع الأجهزة تحت سيطرة البنك فحسب، بل يجب أن تكون هذه الأجهزة صالحة للاستخدام وفقا لطبيعة العمل المصرفي للبنك، وللغرض الذي تم تخصيص هذه الأدوات له[1].

وتعود الخصوصية في مفهوم التزام بائع الأدوات التقنية بالتسليم في مواجهة

---

(١) وعقد بيع الأدوات التقنية هنا يختلف عن عقد نقل التكنولوجيا، ومصدر هذا الاختلاف محل التعاقد في كل من العقدين؛ فعقد نقل التكنولوجيا كما عرفته المذكرة الإيضاحية لقانون التجارة رقم ١٧ لسنة ١٩٩٩ أنه "كل اتفاق يكون محله التزام المورد بنقل معلومات فنية لاستخدامها في إنتاج السلع والخدمات، سواء تعلقت هذه المعلومات بما يعرف بتكنولوجيا المنتج (أي المعرفة التي تستهدف إنتاج منتج معين) أو تعلقت بالتكنولوجية العملية الإنتاجية (التكنولوجية الخاصة بطريقة الإنتاج) ". كما عرف أيضا بأنه عبارة عن عقد يغطى عمليات معينة ويتضمن أداءات محددة تتضمن أخذ أحد الأطراف من الآخر نظاما للإنتاج أو للإدارة، أو خليطا منهما، بموجب تنازل معين وخلال مدة معينة. ومن هذه التعريفات يتضح أن محل عقد نقل التكنولوجيا نقل معارف فنية، من خلال الترخيص باستغلالها مدة معينة وبشروط محددة. أما عقد بيع الأدوات التقنية محله سلع ومنتجات (أجهزة وأدوات) وليس مجرد معلومات تستخدم في إنتاج هذه السلع والمنتجات، كما أنه يؤدى إلى نقل ملكية هذه الأدوات تماما من البائع إلى المشترى (البنك الإلكتروني). لمزيد من التفصيل انظر **إبراهيم المنجي**، مرجع سابق، ص٢٧ وما بعدها. انظر أيضا **د. صلاح الدين جمال الدين**، عقود نقل التكنولوجية، دار الفكر الجامعي، ٢٠٠٥، ص ٢٤.

البنك الإلكتروني، لأمرين:

الأول/ الطبيعة الفنية لشبكة البنك الإلكتروني، والتي ــ كما سبق أن ذكرنا ــ تحتاج إلى أدوات ذات طبيعة خاصة، الأمر الذي يجب معه أن يتم التسليم وفقا للغرض من التعاقد.

الثاني/ الطبيعة الخاصة للعمليات المصرفية، فالأدوات التقنية تتعدد أنواعها وأشكالها، وتتقارب وظائفها وخدماتها، الأمر الذي لا يجعل تحقق استلام البنك لها واستفادته من خدماتها مقصورًا على مجرد حيازتها، بل على تسلمها صالحة للاستخدام وفقا لطبيعة العمل المصرفي للبنك، وللغرض الذي تم تخصيص هذه الأدوات له.

ويترتب على خصوصية مفهوم التزام بائع الأدوات التقنية بالتسليم في مواجهة البنك الإلكتروني أمران:

الأول/ أن يراعي البنك وضع وصف تفصيلي للأدوات التقنية التي يحتاج إليها في العقد الذي يحكم علاقته بمورد الأجهزة، وذلك في ضوء حجم ونوعية الخدمات المصرفية التي سيقدمها(١).

الثاني/ يقتضي الحكم على مدى مطابقة هذه الأدوات التقنية للمواصفات، قيام

(1) (SI will supply all CPUs, communications controllers, DASD equipment, tape/cartridge equipment, printers and related peripheral equipment which may be required for its **operation** of the Data Center as defined in Section 4.1.).**TechAgreement**, data processing,(sector Banking), Exhibit 10.2. term(3.1). available at:http://www.techagreements.com/agreement-review.aspx?num=516688&title=Americorp%20-%20Data%20Processing%20Agreement

البنك بفحصها جيدا، والتأكد من توافر المواصفات المتفق عليها وفقا للعقد المبرم بينه وبين البائع. كما يجب أن يقوم البنك بوضعها تحت التجربة لفترة معينة للتأكد من صلاحيتها وسلامتها. ولعل قيام البنك بعمل محضر تسليم أمر مفيد، وذلك لإبداء التحفظات والملاحظات على التشغيل الأولى، ومدى مطابقة هذه الأدوات للمواصفات المطلوبة [١].

ونرى أن على البنك الإلكتروني ضرورة الاستعانة بفنيين متخصصين عند التعاقد؛ وذلك لانتقاء أفضل أنواع الأجهزة التي تتلاءم مع طبيعة عمل البنك على شبكة الإنترنت، وعند تنفيذ العقد؛ وذلك كي يشرفوا على عملية تسلم هذه الأدوات، حتى يتأكدوا بأنفسهم من توافر المواصفات المطلوبة، سواء من ناحية الكم أم الكيف.

٣٤- ويتفرع عن التزام البائع بتسليم الأدوات التقنية للبنك الإلكتروني، التزام آخر بتسليم ملحقات هذه الأدوات، والتي من أهمها؛ كافة المستندات والوثائق (كتيبات، أسطوانات، دورات تدريبية) الشارحة لنظام عمل هذه الأدوات، سواء ما يجب فعله أم ما يجب الامتناع عن فعله عند استعمال هذه الأدوات، وأيضا أساليب الصيانة الخاصة بهذه الأدوات[٢].

٣٥- يضاف إلى ما سبق وجوب قيام البائع بالتسليم في الميعاد المحدد نظرا لأهمية هذا الأمر؛ حيث إن تسليم هذه الأدوات أمر يتوقف عليه تشغيل البنك

---

(١) د. **محمد حسين منصور**، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، ٢٠٠٣، ص ١٠١.

(٢) المرجع السابق، ص٩٧.

وعمله[1]. وفي مثل هذه الحالات يتم تحديد موعد تقريبي للتسليم، ويجب الالتزام به من قبل البائع كقاعدة عامة، ما لم يقدم مبررات منطقية للتأخير يقدرها قاضي الموضوع، على أن يراعى القاضي طبيعة الالتزام وتعقيداته الفنية. وفي حالة ثبوت تأخير البائع في تسليم المطلوب في الميعاد المحدد تنعقد مسؤوليته عن هذا التأخير، ومن ثم يلتزم بالتعويض عن كل أيام التأخير، مع مراعاة ما أصاب البنك من ضرر من جراء هذا التأخير[2].

(ب) التزام بائع الأدوات التقنية بالإعلام:

٣٦- يعرف الالتزام بالإعلام بأنه عبارة عن التزام الطرف الأكثر خبرة ودراية في العقد، بإعلام وإخبار الطرف الضعيف بكافة البيانات والإرشادات التي تساعد الأخير على استعمال الشيء محل التعاقد وفقا للغرض المخصص له[3].

ويعد الالتزام بالإعلام بالمعنى السابق من أهم الالتزامات الواقعة على عاتق بائع الأدوات التقنية في مواجهة البنك الإلكتروني، وذلك من خلال بتبصير البنك

---

(1) **Chris Reed&John Angel**, Computer law(the law and regulation of information tecnology), Oxford university press, sixth edition,2007, p 183.

(٢) **د.محمد حسين منصور، مرجع سابق، ص ٩٩.**

(٣) **والالتزام بالإعلام، كالتزام يقع على عاتق البائع المهني، لا يجد له أصلا تشريعيا، بل هو من إبداعات القضاء الفرنسي بموجبه يلتزم البائع لمواد ذات طبيعة فنية أو تقنية** بتزويد المستخدم بكافة البيانات والمعلومات التي تمكنه من استعمال الشيء المبيع، وهذا الالتزام يعد **التزاما** تابعا للالتزامات الأصلية الناشئة عن العقد. انظر **عزة محمود أحمد خليل**، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب، رسالة دكتوراه، **كلية الحقوق- جامعة القاهرة**، ١٩٩٤، ص١٢٧؛ **د. نبيلة إسماعيل رسلان**، المسؤولية في مجال المعلوماتية والشبكات، دار الجامعة الجديدة، ٢٠٠٧، ص١٦؛ **د. محمد حسام محمود لطفي**، عقود خدمات المعلومات، القاهرة، ١٩٩٤، ص٩٠.

بكافة الجوانب الخاصة بتشغيل وصيانة الأدوات التقنية الخاصة به.

ويكتسب هذا الالتزام أهمية خاصة في العلاقة بين بائع الأجهزة والبنك، وذلك لسببين(١):

الأول: الطبيعة الفنية المعقدة لمحل العقد. فالأدوات التقنية عبارة عن أجهزة إلكترونية تحتاج إلى علم ودراية بطبيعة الجوانب الفنية الخاصة بها لإمكانية استعمالها، الأمر الذي يربط حسن استفادة البنك من هذه الأدوات بإعلامه من قبل بائع هذه الأدوات بكافة الجوانب الفنية لعمل هذه الأدوات.

الثاني: الطبيعة الخاصة لاعتماد البنك على الأدوات التقنية. فالطبيعة الالكترونية المهيمنة على مجريات النشاط المصرفي للبنك على شبكة الإنترنت تعظم من أهمية إلمام البنك بكافة التفاصيل الفنية الخاصة بعمل الأدوات التقنية، خاصة أن حاجة البنك لمثل هذه البيانات لا تتوقف عند حد الاستخدام الشخصي لها، بل تمتد إلى تمكين البنك من إعلام عملائه بكيفية التعامل مع الأدوات التقنية المملوكة للبنك، والتي يعتمد عليها العملاء في التعامل معه، وذلك على النحو الذي يمكن معه القول بوجوب إعلام البائع البنك بدقائق التفاصيل الفنية المرتبطة بعمل الأدوات التقنية وصيانتها.

وفى سبيل التأكيد على أهمية التزام بائع الأدوات التقنية بإعلام البنك، يذهب جانب من الفقه(٢) إلى أن البائع لا يلتزم فقط بإعلام البنك الإلكتروني بكل التفاصيل الخاصة باستعمال الأدوات التقنية التي قام بتوريدها عند بداية التعاقد،

---

(١) **د. سعيد سعد عبد السلام**، الالتزام بالإفصاح في العقود، دار النهضة العربية، الطبعة الأولى، ٢٠٠٠، ص١١٢.

(٢) **د. محمد حسام محمود لطفي**، مرجع سابق، ص٩٠.

لكن يستمر هذا الالتزام طوال مدة العقد، مادام المستخدم في حاجة للإعلام. وهو ما يطلق عليه جانب من الفقه الالتزام بالتعاون [١]. ويذهب هذا الجانب في سبيل تأصيله لهذا الالتزام إلى القول، بأن العديد من العقود بالإضافة إلى الالتزامات الأصلية التي تتضمنها تنطوي على التزام تبعي بالإدلاء بمعلومات معينة تسمح بحسن تنفيذ الالتزامات القانونية الأصلية، وأن هذا الالتزام التبعي يبرره واجب التعاون والمشاركة بين المتعاقدين لحسن تنفيذ العقد[٢]. وبناء على ذلك يرى هذا الجانب أن مصدر هذا الالتزام (الالتزام بالتعاون) هو العقد، باعتباره من مستلزماته، حيث يلتزم به المتعاقدون كما يلتزمون بالعقد، حتى ولو لم يرد النص عليه صراحة في العقد، على اعتبار أن العقد لا ينفذ فقط طبقا لما ورد فيه، ولكن أيضا وفقا لما تقتضيه قواعد حسن النية، والعرف، والعدالة.

ونحن من جانبنا نتفق مع هذا الجانب من الفقه في جزء، ونختلف معه في جزء آخر؛ حيث نتفق معه في ضرورة التزام المورد في بداية التعاقد بتزويد البنك بكل ما يحتاج إليه من معلومات لازمة لتشغيل الأجهزة والمعدات، وأن هذا الالتزام قائم حتى ولو لم يرد ذكره صراحة في العقد، وذلك باعتباره من مقتضيات العقد في ضوء طبيعة محله والغرض من التعاقد. لكن لا نتفق معه في امتداد هذا الالتزام طيلة مدة تنفيذ العقد إذا لم يرد نص يفصح بذلك صراحة في

(١) ويذهب البعض في تعليل تسمية الالتزام بالتعاون بهذا الاسم إلى أن العميل (البنك الإلكتروني) كما أن له الحق في أن يحصل على كافة المعلومات التي تساعده على التعامل مع الأجهزة، عليه التزام بالتعاون مع المورد، وذلك من خلال إحداث حوار مع المورد، يحدد من خلاله احتياجاته، باعتباره أنه الأكثر قدرة على توصيف هذه الاحتياجات، وتوقع كيفية الحاجة إليها. انظر د. **نبيلة إسماعيل رسلان**، مرجع سابق، ص ٢٠.

(٢) د. **سعيد سعد عبد السلام**، مرجع السابق، ص ١٥

العقد والقول بغير ذلك يعد من وجهة نظرنا اعتداء على مبدأ سلطان الإرادة، هذا المبدأ الذي يعني دائما أن العقد شريعة المتعاقدين، والذي لا يقبل التحايل عليه بدعوى أن العقد ينفذ وفقا لما تقتضيه قواعد حسن النية والعرف والعدالة. فهذه الدعوى هي مجرد وسيلة لتفسير إرادة المتعاقدين دون التحايل عليها.

وبناء عليه يجب على البنك الإلكتروني أن يحرص على أن ينص صراحة في العقد على التزام مورد الأجهزة بتقديم كافة المعلومات اللازمة لتشغيل الأجهزة عند بداية التعاقد، وطيلة مدة تنفيذ العقد. بل نود أن يرتفع مستوى النداء بتوجيهه إلى المشرع المصري للتدخل بنص صريح ينظم من خلاله التزام بائع الأدوات التقنية بإعلام البنك بكافة التفاصيل الفنية الخاصة باستخدام وصيانة هذه الأدوات، وكيفية تنفيذ هذا الالتزام ومدة تنفيذه، على أن يكون نصًا مكملاً لإرادة المتعاقدين، في حالة تغافلهما عن تنظيم هذا الالتزام؛ ويبرر ذلك بأهمية هذا الالتزام بالنسبة للبنك، والذي لا تظهر الأدوات التقنية في نظام عمله مجرد أدوات للحفظ والاسترجاع (كما هو الحال في البنوك التقليدية) ولكنها المحرك الرئيس لنشاطه، سواء على مستوى تواصل العاملين لدى البنك، أم على مستوى تواصله مع العملاء أثناء تقديم الخدمات المصرفية.

٣٧- ويلتزم البنك في المقابل أن يؤدى كافة المستحقات المالية الخاصة بأثمان الأجهزة والأدوات التي تم توريدها، وبالأثمان المتفق عليها، بالإضافة إلى مصاريف التركيب والتشغيل(١).

---

(1) (Client will pay all costs of installing and utilizing communication or telephone lines, data sets, modems, ATMs, terminals, and terminal control units, as required for Client 's on-line operations,

٢)- مسؤولية بائع الأدوات التقنية في مواجهة البنك الإلكتروني:

أ- المسؤولية العقدية لبائع الأدوات التقنية:

٣٨-أشرنا فيما سبق إلى التزام البائع بتسليم الأدوات التقنية المتفق عليها وملحقاتها، طبقا للمواصفات المطلوبة، وفي الميعاد المحدد، كما يلتزم بإعلام البنك بكافة التفاصيل الخاصة باستعمال وصيانة الأدوات التقنية، هذا بالإضافة إلى باقي الالتزامات المقررة في العقد المبرم بينه وبين البنك الإلكتروني.

ويثور تساؤل حول حدود مسؤولية بائع الأدوات التقنية بالتسليم وبالإعلام تجاه البنك الإلكتروني، وكيفية دفعها؟

بخصوص الالتزام بالتسليم يمكن القول من خلال استعراض نص المادتين (٢٠٦، ٤٥٣) من القانون المدني [١] أنهما توحي بأن التزام البائع بالتسليم هو التزام بتحقيق نتيجة. وهذا ما يسرى على التزام بائع الأدوات التقنية في مواجهة البنك، ولكن بالمفهوم الخاص بالتسليم الذي لا يكفى معه مجرد التسليم المادي بوضع الأدوات تحت تصرف البنك، ومن ثم يكتمل التزامه وتنتفي مسؤوليته، ولكن بتمكين البنك من الانتفاع بهذه الأدوات طبقا للمواصفات المتفق عليها، وبما يتلاءم مع الغرض من التعاقد.

وبناء عليه تنعقد مسؤولية البائع العقدية في حالة عدم تحقق الغاية المرجوة من

---

testing and training).**Tech Agreement**, data processing,(sector banking), Op. Cit, term(3.2).

(١) المادة ٢٠٦ " الالتزام بنقل حق عيني يتضمن الالتزام بتسليم الشيء والمحافظة عليه حتى التسليم".المادة ٤٥٣ " التسليم هو وضع المبيع تحت تصرف المشترى بحيث يتمكن من حيازته والانتفاع به دون عائق ولو لم يستول عليه ماديا مادام البائع قد أعلمه بذلك"

التعاقد؛ وذلك كما لو لم يقم البائع بتسليم الأدوات المتفق عليها، أو قام بتسليمها بدون المواصفات المطلوبة. والبنك غير مكلف بإثبات خطأ البائع في هذه الحالة، بل يكفيه فقط إثبات عدم تحقق النتيجة المرجوة، ولا يكفى لدفع مسؤوليته في حالة قيامها، إثبات أنه بذل العناية اللازمة لذلك، بل يجب عليه حتى يتخلص من المسؤولية إثبات السبب الأجنبي.

ويمكن، في حالة امتناع البائع عن تنفيذ أحد التزاماته، أن يتم اللجوء إلى التنفيذ العيني، وذلك في الحدود التي يكون فيها هذا التنفيذ ممكنا، مع الأخذ في الاعتبار الطبيعة الفنية لمحل الالتزام ومدى قابليته للتنفيذ العيني[١].

أما عن التزام بائع الأدوات التقنية بإعلام البنك من خلال تقديم النصائح والإرشادات لإحاطته علما بكافة جوانب تشغيل الأجهزة، فأننا نتفق مع جانب من الفقه[٢] يرى أن هذا الالتزام الأصل فيه أنه التزام ببذل عناية، يتحقق من خلال قيام البائع بجهد مناسب في إعلام البنك، حتى ولو لم يتحقق هذا الإعلام بالفعل. فطبيعة الالتزام بالإعلام يصعب معها القول بأن بائع الأدوات التقنية مكلف بتحقيق نتيجة، باعتبار أن تحقق هذا الالتزام من عدمه يتوقف على عوامل أخرى غير نشاط البائع، كيقظة البنك وتنبهه.

والجدير بالذكر أن معيار بذل العناية (Duty of Care) كوسيلة لقياس الالتزام قد شهد تطورا كبيرا خاصة في معاملات التجارة عبر شبكة الإنترنت، حيث أصبح يحدد في ضوء المخاطر المرتبطة بالنشاط الذي يقوم به الملتزم، بما

---

(١) تنص المادة ١/٢٠٣ من القانون المدني المصري على أن " يجبر المدين بعد إعذاره طبقا للمادتين ٢١٩، ٢٢٠ على تنفيذ التزامه عينيا متى كان ذلك ممكنا" .

(٢) د. **نبيلة إسماعيل رسلان**، مرجع سابق، ص ١٩.

يفرض عليه تحليل المخاطر المحيطة والمتوقعة بالنشاط الملتزم به، ثم يجب عليه بذل عناية تتناسب مع حجم هذه المخاطر، وذلك بمعيار المحترف في أعمال الكمبيوتر والشبكات(١)، الأمر الذي يجعل كل ملتزم في العلاقة قادرا على تحديد الدور المنوط به، ومسؤوليته تجاه هذا الدور، والحد الذي يبدأ عنده الإخلال بالمسؤولية، وذلك في ضوء عناصر واقعية "Real-world" بدلا من التقديرات الجزافية من قبل القضاء "arbitrarily judicial standard"(٢).

---

(1) **Graham Smith**, On- line banking liability, the computer law and security report, 1996, p. 280.

(٢) وقد تم اقتراح هذا المعيار الخاص بتحديد العناية الواجبة في ضوء المخاطر المرتبطة بنشاط الملتزم في مجال التجارة الإلكترونية، ومقدار الثقة المفترضة فيه كنموذج لتطوير المعايير القانونية في مجال المسؤولية في مؤتمر تأمين نظم المعلومات الدولية عام ١٩٩٧ **(National Information Systems Insurance)** وذلك لتفادى عيوب النظام التقليدي (الشخص العادي) في تقدير حدود العناية الواجبة، ومراعاة لتعدد الأطراف الداخلة في علاقات التجارة الإلكترونية.

Amit Yoran, Developing liability standards for electronic commerce, Riptech Security Consulting Group, USA, p2, available at:http://www.isoc.org/inet99/ proceedings/1h/1h_2.htm

- انظر أيضا في ذات المعنى الخاص ببيان طبيعة التزام بائع الادوات التقنية ومقدار العناية التي يجب عليه الالتزام بها؛

(The Supplier warrants that provide the Services efficaciously and in accordance with the highest standard of care that can be reasonably expected of the prudent acting in accordance with all relevant laws, regulations and industry codes of practice, policies and procedures).

Transactional banking services conformed contract, SA Govt transaction banking contract, November 2002, p. 9. .available at:

www.treasury.sa.gov.au/public/download.jsp?id=2481; **Kit Burden**, Electronic commerce proposals-UK, computer law& security report

والملاحظ على هذا المعيار أنه يحدد مقدار العناية المطلوبة في ضوء طبيعة النشاط، وليس كما كان من قبل في ضوء القائم بالنشاط (معيار الشخص العادي). ولعل هذا المعيار الجديد هو الأقرب للعدالة؛ حيث يتسم بالموضوعية، وذلك من خلال تحديد مقدار العناية المطلوبة في ضوء طبيعة الالتزام المفروض، الأمر الذي يؤدى إلى المساواة بين الأشخاص الملتزمين بذات النشاط وإن تعددوا هذا من ناحية. ومن ناحية أخرى يعكس هذا المعيار وجود نوع من التشدد المطلوب في معاملة الملتزمين في تعاملات التجارة الإلكترونية على شبكة الإنترنت. ويبرر ذلك بعظم المخاطر المرتبطة بهذه التجارة خاصة الأنشطة المتعلقة بالبنك الإلكتروني العاملة عبر هذه الشبكة، الأمر الذي يساهم في توفير مناخ قانوني مناسب لهذه البنوك، ومن ثم تقدم التجارة الإلكترونية عبر الإنترنت برمتها.

وبناء عليه يجب ألا يقتصر بذل العناية من قبل بائع الأدوات التقنية في مواجهة البنك على مجرد ترديد إرشادات وتعليمات نصية وحسب، بل يجب عليه أن يبذل كل جهده لإحاطة البنك علما بكافة التفاصيل الخاصة بالتعامل مع الأجهزة والبرامج، مع تقديم الشرح والتدريب الكافي لذلك، ومن ثم تنعقد مسؤولية البائع العقدية إذا أثبت البنك تقصيره في هذا، ويجب على البائع حتى ينفي مسؤوليته أن يثبت أنه بذل العناية الكافية.

والسؤال، هل يسأل بائع الأدوات التقنية عن سلامة الأجهزة والبرامج التي يقوم بتقديمها للبنك ضد المخاطر الناتجة عن استعمالها؟

Vol. 15 no. 4, 1999, p. 250.

٣٩- القول إجابة على هذا التساؤل، أنه لما كان العقد لا يتحدد نطاقه فقط بالالتزامات الصريحة المدونة فيه، وإنما أيضا بما اتجهت إليه نية الأطراف في ضوء طبيعة محل التعاقد، وما استقر عليه العرف في ذلك، إعمالا لنص المادة ١٤٨ من القانون المدني المصري، والتي تقضي بأن (العقد ملزم لأطرافه ليس فقط في حدود ما ورد به من التزامات، ولكن أيضا بما هو من مستلزماته وفقا لقواعد القانون والعرف والعدالة في ضوء طبيعة الالتزام)، فقد استطاع القضاء(١)، وهو في سبيله لتأويل هذا النص، أن يرسى التزاما هاما يقع على عاتق كل شخص محترف يقدم منتجات أو خدمات تنطوي على خطورة ما، بحيث يلتزم به كأحد الالتزامات العقدية حتى ولو لم يرد ذكره صراحة في العقد، وهو الالتزام بالسلامة(٢).

---

(١) **ذهبت المحكمة الاتحادية العليا في دولة الإمارات العربية إلى أن** " لمحكمة الموضوع السلطة المطلقة في تفسير العقود والشروط المختلف عليها بما تراه أوفى لمقصود المتعاقدين مستهدية في ذلك بطبيعة التعامل، وبما ينبغي أن يتوافر من أمانة وثقة بين المتعاقدين، ولا رقابة لمحكمة التمييز عليها في ذلك متى كان تفسيرها مما تحمله عباراتها ولا خروج فيه على المعنى الظاهر وكانت الأسباب التي أوردتها معا من شأنها أن تؤدى إلى النتيجة التي وصلت إليها ..." .**انظر د. نورى حمد خاطر**، مسؤولية المصرف عن الأضرار الناشئة عن استخدام النظام الرقمي في العمليات المصرفية بين المسؤولية المدنية وفعل المباشرة والتسبب، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ هـ ١٠-١٢ مايو ٢٠٠٣ دبي، ص ١٨٠٧.

(٢) وقد كانت بداية الميلاد القانوني لهذا النوع من الالتزام على يد **القضاء الفرنسي** تحت ما يسمى الالتزام بالسلامة في مجال عقود النقل البرى، وذلك تأثرا بوجود هذا الالتزام في عقود النقل الجوى. وقد عمل القضاء بعد ذلك على مد نطاق هذا الالتزام إلى غيرها من عقود المقاولة التي تتناول تقديم نوع من الخدمات تقتضى من المدين اتباع محاذير ومعايير السلامة عند تقديمها، وذلك مثل نشاط أصحاب وكالات السفر والسياحة، وتقديم ألعاب اللهو والترفيه، ومسابقات ركوب الخيل، والمطاعم. انظر د. **فاروق الأباصيرى**، عقد الاشتراك في قواعد المعلومات الإلكترونية، دار النهضة

ويعرف الالتزام بالسلامة بأنه عبارة عن تعهد المدين بتنفيذ العقد دون أن يصيب الدائن بضرر.

ويتطلب الفقه والقضاء[١] لإعمال الالتزام بالسلامة شرطين: الأول / أن ينطوي العقد على خطر يهدد أحد الطرفين. وهذا أمر منطقي يبرر وجود الالتزام بالسلامة. فلولا أن هناك مؤشرات خطرة في طبيعة التزامات المدين ما كان هناك مجال للقول بالالتزام بالسلامة. الثاني/ أن يكون المدين بالالتزام محترفا. ويبرر هذا الشرط أن الالتزام بالسلامة يتطلب من المدين مزيدا من العناية والحرص في تنفيذ العقد، ومن ثم لا يسأل عن هذا الالتزام إلا من كان يتمتع بخبرة عالية تمكنه من بذل العناية والحرص ما لا يقدمه الشخص العادي.

وعند تطبيق ذلك على بائع الأجهزة، نجده ملتزما تجاه البنك بسلامة الأجهزة والمعدات التي يقدمها له ضد المخاطر الناتجة عن استعمالها. فهذا البائع الأصل أنه محترف في طرح هذه المنتجات للتداول (عادة ما تظهر في صورة شركات تجارية)، وأن هذه المنتجات بحسب طبيعة استخدامها، وبحسب البيئة التي ستعمل فيها (شبكة الإنترنت) تنطوي على مخاطر جمة قد تلحق بالبنك،

العربية، ٢٠٠٣، ص ٢١٨؛ **عزة محمود أحمد خليل**، مرجع سابق، ص ١١٨

- وقد أخذ **القضاء الأمريكي** بهذا الاتجاه، حيث ذهب في أحد أحكامه (مسؤولية المورد لا تتوقف على ما علم به أو ما كان يجب العلم به وقت الصنع والبيع وإنما تتوقف على ما ثبت للقضاء من خطورة ما طرح للتداول من منتجات، فالاعتداد بأن حدوث الضرر يمكن أن يكون بطريقة معقولة متوقعا وقت الصنع أو البيع لخفاء الخطر يستتبع استبعاد المسؤولية، بينما التبعات التي تقع على عاتق الصانع في مقابل ما يباشره من نشاط، حماية للغير من التعرض لخطر ملازم لمنتجاته أو جبر الضرر) انظر د. د. **حسن عبد الرحمن قدوس**، مدى التزام المنتج بضمان السلامة في مواجهة مخاطر التطور العلمي، دار النهضة العربية، (بدون تاريخ نشر)، ص٤٣.

(١) **د. نورى حمد خاطر**، مرجع سابق، ص١٨٠٥

خاصة أنه يعتمد عليها بصورة رئيسة في العمل والتواصل مع عملائه، الأمر الذي يجعله مسئولا عن سلامة هذه الأجهزة في مواجهة البنك سواء ورد نص بذلك في العقد الذي يجمع بينهما أم لا. والمسؤولية عن الإخلال بالالتزام بالسلامة مسؤولية مشددة[1]؛ حيث إن البنك غير ملزم بإثبات خطأ البائع كي تقوم مسؤوليته، حيث يكفى وقوع الضرر، كما أن البائع لن يتمكن من دفع مسؤوليته بإثبات أنتفاء الخطأ من جانبه، حيث يجب عليه إثبات السبب الأجنبي.

وعلى الرغم من منطقية هذا الالتزام وعدالته، وما يترتب علي الإخلال به من مسؤولية مشددة تتلاءم مع احتياجات البنك، وذلك على النحو الذي يدفع البائع إلى انتقاء أفضل أنواع الأجهزة التي يزود بها البنك، إلا أن هذه العدالة ذاتها تفرض ألا يكون التزام البائع عن سلامة هذه الأجهزة التزاما مطلقا؛ بمعنى أن هذا الالتزام يجب أن يكون له نهاية يتوقف عندها، ويبدو لنا أن هذه النهاية تبدأ عندما يسيء البنك استخدام هذه الأجهزة عن قصد أو بدون قصد، وذلك على النحو الذي يجعل في استعمالها خطورة عليه، فلا مجال للحديث عن مسؤولية البائع عن سلامة الأجهزة عند عدم اتباع البنك الإرشادات والتعليمات التي أوصاه بها البائع، حيث تبرأ ساحة الأخير في هذه الحالة، والذي سيتمكن من دفع مسؤوليته على أساس توافر السبب الأجنبي؛ وهو عدم وجود علاقة سببية بين نشاطه والضرر الذي وقع للبنك.

ب- المسؤولية التقصيرية لبائع الأدوات التقنية:

٤٠- تقضى قواعد المسؤولية التقصيرية، بأن كل خطأ سبب ضررا للغير يسأل

---

(١) د. محمد عبد الظاهر حسين، المسؤولية القانونية في مجال شبكات الانترنت، دار النهضة العربية، ١٤٢٢هـ - ٢٠٠٢، ص ١١٩

مرتكبه عن تعويض هذا الضرر[1].

وتطبيقا لذلك تنعقد مسؤولية بائع الأدوات التقنية تقصيريا في مواجهة البنك في حالة ارتكابه خطأ غير عقدى يلحق ضررا بالبنك[2]، وذلك كما لو أخبر البنك ببيانات كاذبة عن الأجهزة التي يبيعها له ترتب عليها إبرام العقد. ويجب على البنك إثبات خطأ البائع ليتمكن من الرجوع عليه، ولا يستطيع البائع دفع مسؤوليته إلا بإثبات السبب الأجنبي؛ كالقوة القاهرة مثلا.

٤١- وبعد عرض مسؤولية البائع العقدية والتقصيرية في مواجهة البنك الإلكتروني، تستوقفنا إشكالية تتعلق بعدم كفاية هذه القواعد لمواجهة أشكال المخاطر المختلفة التي يمكن أن تلحق بالبنك الإلكتروني من جراء عمل الأدوات التقنية، خاصة في ظل الاعتماد الكلى للبنك عليها في تقديم خدماته المصرفية للعملاء، وارتباط نجاحه في ذلك ومن ثم الحفاظ على سمعته التجارية وجذب العملاء، على تلافي المخاطر الناجمة عن هذه الأجهزة.

ولفك هذه الإشكالية يمكن القول، بأن السياسة التشريعية في النظم المختلفة ظلت فترة طويلة من الزمن تحتكم إلى فكرة الخطأ كأساس لكلّ من المسؤولية العقدية والتقصيرية. غير أنه مع التطور الذي لحق أسلوب وأدوات تنفيذ الالتزامات القانونية؛ من خلال الآلات الميكانيكية تارة والآلات الإلكترونية تارة أخرى، ظهر اتجاه يسعى إلى استحداث أساس آخر للمسؤولية يقوم على فكرة المخاطر؛ إذ يكفى لقيام المسؤولية عن الضرر أن يكون نشاط الملتزم ينطوي

(١) المادة ١٦٣ من القانون المدني المصري، والمادة ١٣٨٢ فرنسي.

(2) **Graham Smith**; Op. Cit, p. 279

على خطورة ما، حتى ولو لم يصل هذا النشاط إلى حد الخطأ[1]، بمعنى أن هذه المسؤولية تقوم على ركنين فقط؛ هما الضرر وعلاقة السببية. ويطلق على هذا النوع من المسؤولية؛ المسؤولية الموضوعية أو تحمل التبعة.

ويتميز هذا النوع من المسؤولية- بالمقارنة بالمسؤولية عن المخاطر الناشئة عن الالتزام بالسلامة سالف الذكر- أن كلاً من البنك وعملائه يستطيعون الاستفادة منه في الرجوع على بائع الأدوات التقنية، وذلك بالنظر إلى أنه لا يتطلب وجود عقد تمت مخالفة التزاماته، ولا يتطلب وجود خطأ من جانب البائع في تنفيذ أحد التزامات هذا العقد، بل يكفى أن يكون نشاط البائع سبب ضررا للبنك أو عملائه.

وتجد هذه النظرية مبررات تطبيقها لدى البعض[٢] في صعوبة إثبات الخطأ في مجال المعاملات الإلكترونية؛ حيث يتعذر على المضرور اكتشاف الأخطاء التي يؤسس عليها دعواه. يضاف إلى ذلك من تبرير، أن العدالة تقتضى ألا يحرم المضرور من التعويض لمجرد عدم صدور خطأ من المتسبب.

ونرى أن هذه التبريرات لا تقوى على حمل هذه النظرية، التي باتت تلعب دورا هاما في مواجهة الأضرار الناجمة عن المعاملات الإلكترونية على شبكة الإنترنت، خاصة إذا تعلق الأمر بالمعاملات المصرفية، والتي تحتاج إلى مستوى أعلى من الحرص، يتبعه تشديد أكبر في المسؤولية. فالمعاملات الإلكترونية شهدت تطورا كبيرا، على النحو الذي لم يعد يقبل معه القول بوجود صعوبة في

---

(1) **Amit Yoran**; Op. Cit, p. 2.

(٢) د. **شريف محمد غنام**، مسؤولية البنك عن أخطاء الكمبيوتر في النقل الإلكتروني للنقود، دار النهضة العربية، بدون تاريخ نشر، ص ٩٥.

إثبات هذه المعاملات، وإثبات الأخطاء الناجمة عنها، الأمر الذي أدركته العديد من التشريعات، وأضحت تضفى الحجية على المخرجات المختلفة للوسائل الإلكترونية، بل وسعت إلى التشديد على أهمية الالتزام بإعلام المستخدم (البنك الإلكتروني) بالجوانب الفنية الخاصة باستعمال الأجهزة الإلكترونية التي يقوم بتوريدها، الأمر الذي يؤهل المستخدم للإحاطة بالعديد من هذه الجوانب، وذلك على النحو الذي يسهل عليه بعد ذلك إثبات ما بها من خلل أو أعطال. أيضا فكرة العدالة لا يستقيم معها القول بتحميل أحد الأطراف المسؤولية عن كافة الأضرار لمجرد أنه أعتمد على الوسائل الإلكترونية في أداء نشاطه، وذلك دون مراعاة لإهمال أو تقصير الطرف المناظر له عند التعامل مع هذه الوسائل الإلكترونية.

وتجد هذه النظرية تبريرها لدينا؛ في خطورة عمل الأجهزة الإلكترونية على شبكة الإنترنت، خاصة في المعاملات المصرفية، وذلك في ظل عدم تساوى مراكز الأطراف المتعاقدة في الإلمام بالفنيات والتعقيدات الخاصة بعمل هذه الأجهزة؛ فمورد الأجهزة والأدوات الإلكترونية في مركز أقوى من البنك؛ من حيث الإلمام بتفاصيل عمل هذه الأدوات؛ سواء فيما يتعلق بتشغيلها، أو تجنب أعطالها، وكيفية صيانتها، الأمر الذي يبرر حرصا أكبر من قبل مورد الأجهزة، على النحو الذي يجعله مسئولا ليس فقط عن الأضرار الناجمة عن خطأه (بالمعنى المقرر في المسؤولية العقدية والتقصيرية)، ولكن أيضا عن الأضرار الناتجة عن نشاطه، على أن تتوقف حدود هذه المسؤولية عند حد وجود السبب الأجنبي (كالقوة القاهرة والحادث الفجائي).

هذا وقد جاء النظام القانوني المصري خلوا من نص خاص ينظم المسؤولية على أساس المخاطر.

وقد كان للفقه الإسلامي فضل السبق في صياغة هذه النظرية، حيث لا يشترط وفقا لهذا الفقه وجود تعد لجبر الضرر (لإقامة المسؤولية)، فالعبرة بالضرر لا بالفعل ذاته [1].

ولقد ورد أساس هذه المسؤولية أيضا في التوجيه الأوربي الصادر عام ١٩٨٥، الذي تم تنفيذ أحكامه في فرنسا بمقتضى القانون الصادر عام ١٩٩٨ بخصوص قواعد المسؤولية عن المنتجات المعيبة، حيث جعل أساس المسؤولية عن هذه المنتجات، هو ما تتضمنه من عيوب تشكل خطورة على الشخص المستخدم لها، وتلحق به ضررا سواء كانت هناك رابطة عقدية أم لا [2].

ولقد فطن القضاء الأمريكي لهذا الاتجاه، وذلك عندما أدرك عدم كفاية قواعد المسؤولية العقدية (القائمة على أساس الإخلال بالتزام اتفاقي)، وقواعد المسؤولية التقصيرية (القائمة على أساس الإخلال بواجب قانوني عام) على مواجهة ما يلازم مخاطر التطور العلمي، لذا أخذ على عاتقه مع مستهل القرن العشرين بناء نظام قانوني موضوعي لجبر الضرر [3].

ويترتب على ذلك، القول بأن بائع الأدوات التقنية يسأل في مواجهة البنك الإلكتروني عن كافة الأضرار الناجمة عن استخدام هذه الأدوات بسبب نشاطه، حتى ولو لم يصل هذا النشاط إلى حد الخطأ (عقدي أو تقصيري).

ويبدو لنا أن هذا نوع من التشدد في مسؤولية البائع، لكنه تشدد تبرره درجة اعتماد البنك الإلكتروني وحاجته الملحة لهذه الأجهزة، فالأجهزة والأدوات التقنية

---

(١) د. **نورى حمد خاطر**، مرجع سابق، ص١٨٣٣.
(٢) د. **فاروق الأباصيرى**، مرجع سابق، ص٢١٨.
(٣) د. **حسن عبد الرحمن قدوس**، مرجع سابق، ص٥٦

في حياة البنك الإلكتروني ليست مجرد وسيلة لتحسين أداء الخدمة، أو التسهيل على العملاء، لكن المسألة مرتبطة بوجود البنك من غدمه.

٣)- مسؤولية بائع الأدوات التقنية في مواجهة عملاء البنك الإلكتروني:

٤٢- طبقا للقواعد العامة في المسؤولية المدنية، فأن عميل البنك الإلكتروني لا يملك الرجوع مباشرة على بائع الأجهزة بموجب قواعد المسئولية العقدية، حيث إن العميل ليس طرفا في عقد البيع. بيد أن العميل يملك الرجوع على بائع الأجهزة بموجب قواعد المسؤولية التقصيرية إذا تمكن من إثبات خطأ البائع المتسبب في إلحاق الضرر به. ويمللك العميل كذلك الرجوع على البائع حتى لو لم يصدر خطأ من الأخير، وذلك بموجب قواعد المسؤولية الموضوعية (تحمل التبعة)، تلك التي تجعل البائع مسئولاً عن الضرر الناتج عن نشاطه، حتى ولو لم يرقى هذا النشاط إلى درجة الخطأ؛ باعتباره يقدم أجهزة ذات طبيعة خاصة، يترتب على استعمالها مخاطر.

والسؤال هل يملك العميل الرجوع على البنك الإلكتروني في حالة إصابته بضرر ناجم عن الأدوات التقنية التي يتعامل معها للحصول على الخدمات المصرفية؟

٤)- مسؤولية البنك الإلكتروني عن أضرار الأدوات التقنية في مواجهة العميل:

٤٣- يسأل البنك الإلكتروني عن الأضرار الناجمة عن الأدوات التقنية في مواجهة العميل في الحالات الآتية:

الأولى: بموجب قواعد المسؤولية العقدية، وذلك إذا تضمن العقد المبرم بينهما ما

يفيد التزام البنك بسلامة الأدوات التقنية التي يتعامل معها العميل للحصول على الخدمة المصرفية[1]. بل يمكن القول بأن البنك مسئول عقديا عن سلامة هذه الأدوات، حتى ولو لم يرد نص صريح بذلك في العقد[2]. ويتأسس هذا الالتزام في هذه الحالة على حكم المادة ١٤٨ من القانون المدني المصري. وتبرير ذلك أنه لما كان العقد المصرفي عبر شبكة الإنترنت، والذي يحكم علاقة البنك بالعميل ينطوي على خطورة مصدرها الطبيعة الفنية المعقدة للأدوات التقنية المستخدمة في تقديم الخدمة، يضاف إلى ذلك طبيعة المدين بالالتزام (البنك الإلكتروني) من كونه محترفا في تقديم الخدمة المصرفية، ومن ثم ينتظر منه أكثر مما ينتظر من الآخرين من عناية وحرص[3]، فأن البنك يسأل عن سلامة هذه الأدوات، حيث يعد الالتزام بالسلامة في هذه الحالة التزاما عقديا ثانويا يلتزم به البنك في مواجهة عميله.

لكن إلى أي درجة يلتزم البنك بسلامة وكفاءة هذه الأجهزة في علاقته بالعميل؟ بمعنى آخر هل التزام البنك التزام ببذل عناية أم بتحقيق نتيجة؟

من خلال مطالعة معظم العقود المصرفية التي تحكم علاقة البنك العامل على شبكة الإنترنت بعملائه، نلاحظ أن الصيغة التي تتضمنها هذه العقود تفيد قصر مسؤولية البنك على مجرد بذل عناية معقولة، وأنه غير مسئول عن أية أخطأ تحدث بسبب تقديم الخدمة، سواء كانت هذه الأخطاء تعود للأجهزة

---

(1) **Graham Smith**; Op. Cit, p. 277.

(٢) د. **شريف محمد غنام**، مسؤولية البنك عن أخطاء الكمبيوتر في النقل الإلكتروني للنقود، مرجع سابق، ص٢٨ وما بعدها.

(٣) د. **محمد عبد الظاهر حسين**، مرجع سابق، ص ١١٨.

والبرامج الخاصة بالبنك، أم تعود لمقدمي الخدمات الإلكترونية(1).

ويبدو لنا أن هذا القدر من المسؤولية لا يتناسب مع طبيعة الخدمة المصرفية التي تقدم عبر شبكة الإنترنت، تلك الخدمة التي تفرض على البنك مزيدا من الجهد والحرص عند تقديم الخدمة لعملائه، بما يستتبع ذلك ضمان كفاءة وسلامة الأجهزة المسئولة عن تقديم هذه الخدمة، وذلك على النحو الذي لا يقبل معه القول بأن على البنك أن يبذل عناية معقولة في هذا الصدد؛ بل أن طبيعة الخدمة المصرفية، وطبيعة البيئة التي تقدم فيها (شبكة الإنترنت) تفرض على البنك الالتزام بتحقيق نتيجة تتمثل في ضمان كفاءة وسلامة الأجهزة التي يستخدمها في تعامله مع العملاء، بما يفرض عليه انتقاء أفضل أنواع الأجهزة والتأكد من سلامتها. ويقتضى هذا القدر من المسؤولية افتراض خطأ البنك في حالة عدم تحقق النتيجة المرجوة، وذلك على النحو الذي لا يجعل العميل مكلفا بإثبات خطأ البنك، ولا يكون أمام الأخير لدفع مسؤوليته في هذه الحالة سوى إثبات السبب الأجنبي.

الثانية: يمكن للعميل الرجوع على البنك بموجب قواعد المسؤولية التقصيرية إذا

---

(1) (While the Bank will make reasonable efforts to provide the Service, the Bank will not be liable for any failure to provide the Service or any part of the Service for any cause that is beyond the Bank's reasonable control including, in particular, any suspension of the Service resulting from maintenance and up grades to the Bank's systems or those of any other party used to provide the Service).

JYSKE BANK, Jbpb, Net Bank user agreement, (EN)-2007, available at: http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf

ما صدر عن البنك خطأ سبب ضررا للعميل خارج نطاق الالتزامات العقدية(١).

الثالثة: رجوع العميل على البنك على أساس نظرية تحمل المخاطر. وهذا ما ذهب إليه فريق من الفقه(٢) نؤيده. ويبرر هذا الجانب موقفه بالقول بأن البنك اعتمد على التكنولوجيا الحديثة لتقديم خدماته للعملاء، وهذه التكنولوجيا أمر معقد بالنسبة لغير المتخصص (العميل)، كما أنها تنطوي على مخاطر غير عادية، ومن ثم من العدل أنه كما أن البنك يستفيد من هذه التكنولوجيا، فعليه أن يتحمل تبعة مخاطرها. نضيف إلى ذلك أن توسيع قاعدة المسؤولية أمام العميل، من خلال إدخال البنك الإلكتروني في نطاقها- حتى ولو لم يثبت الخطأ من جانبه- من شأنه أن يزيد من طمأنينة العميل وارتياحه في التعامل مع البنك الإلكتروني العامل عبر شبكة الإنترنت.

لكن السؤال هل يمكن للعميل أن يعود على البنك بوصفه حارسا للأشياء، ومن ثم يعد مسئولاً عما تحدثه الأدوات التقنية من ضرر للعميل؟

٤٤- نص القانون المدني المصري في المادة ١٧٨ منه على أن " كل من تولى حراسة أشياء تتطلب حراستها عناية خاصة أو حراسة آلات ميكانيكية يكون مسئولا عما تحدثه هذه الأشياء من ضرر، ما لم يثبت أن وقوع الضرر كان بسبب أجنبي لا يد له فيه" (٣).

---

(1) **Graham Smith**; Op. Cit, p. 277.

(٢) **د. نوري حمد خاطر**، مرجع سابق، ص ١٨٣.

(٣) ويعد هذا النص ترجمة حقيقية لإدراك المشرع المصري أهمية الأدوات الميكانيكية (واستشرافه لأهمية الأدوات الالكترونية) في تنفيذ الالتزامات القانونية خاصة بعد ظهور شبكة الانترنت وانتشار الممارسات التجارية عليها، والتي تعتمد اعتمادا كلية سواء في المراحل الأولى للتعاقد أو أثناء تنفيذه أو حتى فض المنازعات الخاصة به

وقد وضع هذا النص شرطين لقيام مسؤولية حارس الأشياء عن الضرر الذي تحدثه: الأول: وجود حراسة على الشيء يملك بموجبها الحارس استعمال سلطات الرقابة والتوجيه والاستعمال. الثاني: التدخل الإيجابي لهذا الشيء لإحداث الضرر، حيث لا يكفى التدخل السلبي، ويجب على المضرور إثبات هذا التدخل[1]:

وقبل أن نقرر انطباق النص السابق على البنك الإلكتروني يثور تساؤلان؛ الأول يتعلق بمدى اعتبار البنك حارسا في ضوء نص المادة ١٧٨ من القانون المدني؟ والثاني بمدى اعتبار الأجهزة والبرامج التي يتعامل بها البنك مع عملائه من قبيل الآلات الميكانيكية أو الأشياء التي تتطلب حراستها عناية خاصة؟

أولا/ مدى اعتبار البنك الإلكتروني حارسا:

من خلال استقراء نص المادة ١٧٨ سالفة الذكر، يلاحظ أن المشرع المصري لم يحدد المقصود بالحراسة، ولا من هو الحارس، الأمر الذي فتح باب الاجتهاد للفقه والقضاء في تحديد المقصود بالحراسة.

وقد تبنى الفقه والقضاء في البداية نظرية الحراسة القانونية؛ تلك التي تقضى بأن الحارس هو الشخص صاحب السلطة القانونية على الشيء بموجب ما له من

المعاملات (التحكيم الإلكتروني) على الأدوات الإلكترونية، الأمر الذي جعل المشرع يستشرف هذه الرؤى في نطاق نص المادة ١٧٨ سالف الذكر ليقر بمسؤولية متولي الرقابة على هذه الأدوات عما تحدثه من ضرر، وذلك من أجل أن يهتم متولي الرقابة بانتقاء هذه الأدوات، والحرص على الإلمام بكافة الجوانب الخاصة بعملها وتشغيلها تفاديا لكل ما يمكن أن ينتج عنها من أضرار.

(١) د. **أحمد شوقي عبد الرحمن**، النظرية العامة للالتزام (مصادر الالتزام)، دار القلم للنشر والتوزيع، ٢٠٠٠، ص٣٢٩.

حق عيني أو شخصي عليه بناء على عقد أو نص في القانون. لكن سرعان ما توارت هذه النظرية على أثر ما وجه إليها من انتقادات، تعلقت بغياب الأساس القانوني السليم لربط الحراسة بوجود سلطة قانونية على الشيء؛ فقد يسرق الشيء من مالكه[1]، فكيف يسأل الأخير عن ما يحدثه هذا الشيء من أضرار وهو تحت سيطرة السارق.

وسرعان ما تحول الفقه[2] والقضاء[3] على أثر هذه الانتقادات إلى الأخذ بنظرية الحراسة الفعلية؛ تلك التي تقضي بأن الحارس هو الشخص صاحب السلطة الفعلية على الشيء، على نحو يمكنه من استعماله وتوجيهه والرقابة عليه، وذلك لحساب نفسه أي بصورة مستقلة.

ومن خلال النظر في وضع البنك الإلكتروني نلاحظ أنه يعتبر حارسا وفقا لنص المادة ١٧٨ سالفة الذكر، يستوي في ذلك الأخذ بنظرية الحراسة القانونية أو الفعلية؛ فالبنك حارس قانوني بموجب ما له من حق ملكية على الأجهزة الإلكترونية التي في حوزته، كما أنه صاحب حراسة فعلية عليها بموجب تواجد هذه الأجهزة في حيازته وخضوعها لاستعماله وتوجيهه ورقابته بصورة مستقلة.

---

(١) د. **محمد لبيب شنب**، المسؤولية عن الأشياء (رسالة دكتوراه)، مكتبة النهضة المصرية، ١٩٥٧، ص ٧٧

(٢) د. **محسن عبد الحميد البيه**، النظرية العامة للالتزام (المصادر غير الإرادية) دار النهضة العربية، ٢٠٠٨، هامش ص ٢٠٩.

(٣) **ذهبت محكمة النقض المصرية إلى " أن نص المادة ١٧٨ من القانون المدني يدل على أن الحراسة على الأشياء الموجبة للمسئولية على أساس الخطأ المفترض طبقا لهذا النص تتحقق بسيطرة الشخص الطبيعي أو المعنوي على الشيء سيطرة فعلية من خلال الاستعمال والتوجيه والرقابة لحساب نفسه"** راجع نقض مدني مصري، ١٧/ ١٢/ ١٩٩٥، طعن ٥٥٤، س ق ٥٩، قاعدة ٢٧٤، مجموعة أحكام النقض (الجزء الثاني)، ص ١٣٩٦.

وبناء عليه ينطبق على البنك الإلكتروني وصف الحارس وفقا لنص المادة ١٧٨ من القانون المدني.

ثانيا/ مدى اعتبار الكمبيوتر من قبيل الآلات الميكانيكية أو الأشياء التي تحتاج لعناية خاصة:

عرفت اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري(١) في المادة (١) الكمبيوتر بأنه عبارة عن "جهاز إلكتروني قادر على تخزين ومعالجة وتحليل البيانات والمعلومات بطريقة إلكترونية".

كما تعرض الفقه - في ظل غياب نص قانوني - لتعريف الآلات الميكانيكية، فذهب البعض(٢) إلى أنها عبارة عن "الأشياء التي تدار بمحرك ذاتي أيا كان نوعها، وأيا كان مصدر الطاقة التي تحركها، كالكهرباء أو الماء أو البخار أو الهواء أو البترول أو الطاقة الشمسية"، وذهب البعض الآخر(٣) إلى أنها عبارة عن "مجموعة من الأجسام الصلبة، الغرض منها تحويل عمل إلى عمل آخر، وهي تستمد حركتها من محرك أو قوة دافعة، غير الإنسان، سواء كانت البخار أو الكهرباء أو المياه أو الهواء، ولا يهم الغرض الذي تستعمل من أجله الآلة، ولا المواد المصنوعة منها، ولا الشكل الذي تتخذه، سواء كانت من العقارات أم من المنقولات".

ومن خلال مضاهاة هذه التعريفات، يتبين لنا أن تعريف الآلات الميكانيكية

---

(١) انظر: **الوقائع المصرية**، العدد ١١٥ (تابع)، ٢٥ مايو ٢٠٠٥

(٢) د. **شريف محمد غنام**، مسؤولية البنك عن أخطاء الكمبيوتر في النقل الإلكتروني للنقود، مرجع سابق، ص٦٨

(٣) د. **محمد لبيب شنب**، مرجع سابق، ص ٥٤

قريب من تعريف الكمبيوتر، حيث إنها كلها مجموعة من الأشياء تعمل بالطاقة بهدف تحقيق نتائج معينة، إلا أن ذلك لا يعنى التسليم بأن الكمبيوتر يعد من الآلات الميكانيكية؛ حيث إن الأخيرة تقوم على فكرة استخدام الطاقة بهدف الدفع والحركة (Power)[(١)]، وذلك على عكس الكمبيوتر الذي يقوم على فكرة استخدام الطاقة بهدف معالجة البيانات للتوصل إلى نتيجة معينة، الأمر الذي يجعلنا لا نميل إلى القول بأن الكمبيوتر من الآلات الميكانيكية في حكم نص المادة ١٧٨ سالفة الذكر.

أما من ناحية مدى اعتبار الكمبيوتر من قبيل الأشياء التي تحتاج إلى عناية خاصة، فالملاحظ أن الفقه قد اختلف على نفسه في تحديد المقصود بالأشياء التي تحتاج إلى عناية خاصة إلى رأيين:

الرأي الأول: يرى أن الشيء يحتاج إلى عناية خاصة (ومن ثم يخضع لنص المادة ١٧٨ سالفة الذكر) عندما يكون خطرا بطبيعته، بغض النظر عن طريقة استعماله، أو الظروف التي تم استعماله فيها. ومثال على ذلك المتفجرات والذخائر[(٢)].

الرأي الثاني: يرى أن الشيء يحتاج إلى عناية خاصة عندما يكون خطرا بطبيعته وخطرا بحسب طريقة استعماله أو الظروف التي تم استعماله فيها.

---

(١) ومن أمثلة الآلات الميكانيكية الدراجات البخارية، والسيارات والطائرات والسفن والآلات الزراعية. ويجب أن نشير إلى توصيف شيء ما بأنه من قبيل الآلات الميكانيكية من عدمه أمر تقرره محكمة الموضوع تحت إشراف ورقابة محكمة النقض باعتبار أنها مسألة قانون، وذلك لارتباط هذا الوصف بركن من أركان المسؤولية عن حراسة الأشياء. انظر د. **محسن عبد الحميد البيه**، مرجع سابق، هامش ص ٢٠٩.

(٢) د. **محمد لبيب شنب**، المسؤولية عن الأشياء، مرجع سابق، ص ٦٩.

ومثال على هذه الأشياء؛ الشجرة التي توضع في أرض زراعية لا تشكل خطورة، لكن لو وضعت ذات الشجرة على طريق للمارة أو السيارات فهي خطرا بالنظر إلى احتمالية اقتلاعها بفعل الرياح فتهدد حياة المارة [١]. وهذا ما أخذت به محكمة النقض المصرية [٢].

ويبدو لنا أن الرأي الثاني أقرب إلى الصواب في فهم المقصود بالأشياء التي تحتاج إلى عناية خاصة وفقا لنص المادة ١٧٨. وذلك لأنه حتى الشيء الذي يعد بطبيعته خطرا وفقا للرأي الأول فأن هذه الخطورة لا تظهرّ إلا بحسب طريقة استعمال الأشياء والظروف التي تستعمل فيها. وبناءً عليه نرى أن الكمبيوتر والبرامج المثبتة به تعد أشياء تحتاج إلى عناية خاصة، وذلك بالنظر إلى طبيعتها وطبيعة البيئة التي تعمل فيها؛ فالكمبيوتر على الرغم من الدقة المتناهية التي يمكن أن يصل إليها في تنفيذ العمليات المطلوبة منه، إلا أنه يمكن أن يأتي بنتائج عكس ذلك تماما إذا أخطأ أو نسى من يدخل إليه الأوامر في مجرد الضغط على أحد مفاتيح التشغيل، الأمر الذي يلوح بالمخاطر التي يمكن أن تنتج عن استعماله، ومن ثم العناية الخاصة التي يحتاج إليها لتفادى هذه المخاطر. يضاف إلى ذلك، الغرض الذي يتم من أجله استعمال هذه الأجهزة؛ وهو تقديم الخدمات المصرفية وما يحتاجه ذلك من دقة وعناية بالغة، وأخيرا البيئة التي يعمل فيها البنك (شبكة الإنترنت) من كونها بيئة للاتصال الإلكتروني

---

(١) انظر د. **شريف محمد غنام**، مسؤولية البنك عن أخطاء الكمبيوتر في النقل الإلكتروني للنقود، مرجع سابق، ص ٦٨، ٦٧، د. **محسن عبد الحميد البيه**، مرجع سابق، ص ٢١٠.

(٢) **نقض مدني مصرى**، ١٩٨٩/١/١٥، طعن١٧٨١، س ق ٥٦، القاعدة (٣٢)، مجموعة أحكام النقض (الجزء الأول)، س ٤٠، ص ١٤٥.

مفتوحة على العالم بأسره، الأمر الذي يؤكد أن هذه الأشياء تحتاج إلى عناية خاصة.

وبناء عليه يمكن القول برجوع العميل على البنك بموجب قواعد المسؤولية عن حراسة الأشياء غير الحية، حيث يسأل الأخير في مواجهة الأول عما تسببه الأجهزة الخاصة بالبنك والتي توجد تحت حراسته. ولا يكلف العميل في مثل هذه الحالة بإثبات خطأ البنك حيث أنه مفترض، ولا يستطيع البنك أن يدفع مسؤوليته بإثبات عدم صدور خطأ من جانبه، أو بانتفاء العلاقة بين خطئه والضرر، بل يجب عليه في هذه الحالة إثبات السبب الأجنبي؛ كقوة قاهرة، أو انقطاع علاقة السببية بين الضرر وفعل الأجهزة (كما لو لم يكن تدخل الأجهزة تدخلاً إيجابيًا لإحداث الضرر).

وأخيرا لا شك أن تعدد صور مسؤولية البنك في مواجهة العميل من شأنها تشجيع هذا العميل على التعامل مع البنك، وذلك في ظل حداثة العمل المصرفي على شبكة الإنترنت، وفي ظل كثرة المخاطر التي تحيط به، حيث إن هذا التعدد من شأنه أن يزيد من ضمانات العميل في مواجهة البنك، من خلال تغطية معظم صور المخاطر الناجمة عن تعاملاته مع البنك، بما يزيد من طمأنينة العميل ويشجعه على التعامل مع البنك، بما ينعكس على ربحية البنك ونجاحه.

ثانيًا- الحصول على المكونات المعنوية اللازمة لشبكة البنك:

٤٥- يشكل حصول البنك على المكونات المعنوية اللازمة لإنشائه أهمية كبيرة؛ باعتبار أن هذه المكونات هي المسئولة عن ربط عمل المكونات المادية وتنظيم عملها المصرفي بشكل متناسق.

وتعرف المكونات المعنوية اللازمة لشبكة البنك الإلكتروني بأنها مجموعة البرامج المعلوماتية المصممة من قبل مبرمجين متخصصين، لتحكم وتنظم عمل وتشغيل المكونات المادية للشبكة الداخلية للبنك على الإنترنت(١).

وقد عرفت اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري(٢) في المادة (١) البرنامج المعلوماتي بأنه عبارة عن "مجموعة أوامر وتعليمات معبر عنها بأية لغة أو رمز أو إشارة، وتتخذ أي شكل من الأشكال، ويمكن استخدامها بطريقة مباشرة أو غير مباشرة في حاسب آلي لأداء وظيفة أو تحقيق نتيجة، سواء أكانت هذه الأوامر والتعليمات في شكلها الأصلي، أم في شكل آخر تظهر فيه من خلال الحاسب الآلي"

ومن ناحيتها فقد عرفته المنظمة العالمية للملكية الفكرية(٣) بأنه عبارة "عن مجموعة معارف أو معلومات يعبر عنها في شكل شفوي أو مكتوب أو بيانى أو غيره، يمكن نقلها أو تحويل صورتها بفك رموزها بواسطة آلة يمكن أن تنجز مهمة أو تحقق نتيجة محددة بواسطة جهاز إلكتروني أو ما يماثله يمكنه القيام بتحقيق عمليات معقدة تهدف لغايات عملية".

---

(1) **M.Sklira – A.S. spomportsis – M.S. obaidat**; Op. Cit., p. 1776.
- انظر أيضا د. **خالد مصطفى فهمي**، مرجع سابق، ص ٩.

(٢) انظر: **الوقائع المصرية**، العدد ١١٥ (تابع)، ٢٥ مايو ٢٠٠٥

(٣) أشار إلى هذا التعريف د. **محمد عبد الظاهر حسين**، الاتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية، دار النهضة العربية، ٢٠٠٠ -٢٠٠١، ص٩.
- وقد عرف قانون حقوق تأليف برامج الكمبيوتر الأمريكي الصادر عام ١٩٧٦ والمعدل في ١٩٨٠ البرنامج المعلوماتى بأنه عبارة عن (مجموعة البيانات أو الأوامر التي تستخدم بشكل مباشر أو غير مباشر في الحاسوب للوصول إلى نتيجة محددة).

Roger Gerleroy Miler – Gaylord A. Jentz; Op. Cit, p. 116.

وتوجد عدة طرق قانونية يمكن للبنك من خلالها الحصول على البرامج المعلوماتية اللازمة له:

١) عقد بيع البرامج المعلوماتية:

٤٦- وفي سبيل حصول البنك الإلكتروني على البرامج المعلوماتية اللازمة لتشغيله، فأن عليه التعاقد عليها بالبيع ممن له الحق في التصرف فيها، بالكميات والمواصفات اللازمة لطبيعة عمل البنك. لكن هذا البيع ذو طبيعة خاصة[١]، حيث إن الملكية التي تنتقل للبنك الإلكتروني بموجبه، هي ملكية الوسيط المادي (الاسطوانة، الكمبيوتر) المحمل عليه البرنامج[٢]، دون البرنامج ذاته، حيث يظل ملكا لمؤلفه[٣] (صاحب حق الملكية الفكرية)[٤]، وإن حصول البنك الإلكتروني

---

(١) د. محمد حسين منصور، مرجع سابق، ص ٣٧.

Graham Smith; Op., Cit, p. 279.

(2)**Michael P. Dierks**, Computer network abuse, Harvard journal of law, Volume 6, Spring Issue, 1993, p 322

(٣) ويعرف **مؤلف البرنامج المعلوماتي** بأنه الشخص الطبيعي أو المعنوي، أو مجموعة الأشخاص الذين قاموا بتصميم (created) هذا البرنامج. والقانون يعطي الحماية لهذا المؤلف متى كان هو المؤلف الحقيقي للبرنامج، ومتى قام بإخراج هذا المؤلف في شكل مادي وملموس (أي لا تكون مجرد أفكار حبيسة نفسه).

Legal protection, Computer programs, available at: http://eurOpa.eu/scadplus/leg/en/ lvb/l26.27.htm; **Edward J. Obloy and B. Helen Sharetts-Sullivan**, Exploitation of Intellectual Property by electronic chartmakers: liability, Retrenchment and a Proposal for Change, Defense mapping agency, p 4. available at: http://www.spatial.maine.edu/~onsrud/tempe/obloy.html

(4)**Julian JB Hickey – Robin Mathew-ChristOpher**; Op. Cit, p. 121;

على نسخة من هذا البرنامج مقابل دفع ثمنها، إنما هو لاستعماله فقط، دون استغلاله؛ من خلال إعطاء نسخة منه للعملاء مثلا [(١)].

ويسرى على هذا البيع ذات القواعد السابق الحديث عنها بخصوص عقد بيع الأدوات التقنية، من حيث التزام البائع بالتسليم طبقا للموصفات المتفق عليها، بالإضافة لالتزامه بإعلام البنك بكافة الجوانب الخاصة باستعمال هذه البرامج[(٢)].

٢)- حصول البنك الإلكتروني على الحق في استغلال البرنامج:

٤٧- أتضح من خلال التعرض لحصول البنك الإلكتروني على البرنامج

William Gram, Legal Analysis of a Banking Industry Online Identity and Attribute Authentification Service for Consumers and Merchants: The Financial Service Technology Consortium's FAST Initiative, Federal Reserve Bank of Chicago, 2000, p. 24.

- وقد حرصت العديد من التشريعات على التأكيد على حماية حقوق مؤلف البرنامج على مصنفه عبر شبكة الانترنت، وأن كانت قد ربطت هذه الحماية بضرورة قيام مؤلف البرنامج بمراعاة الضوابط المتعلقة بتسجيل هذا المصنف لدى الجهات المختصة بذلك. وقد فرض قانون الملكية الفكرية الأمريكي على مؤلف البرنامج ضرورة مراعاة إجراءات التسجيل لدى مكتب التسجيل الخاص بحقوق الملكية الفكرية **(U.S. Copyright Office)**، ولا يسمح لأحد بأن ينتفع بهذا المصنف إلا وفقا لترخيص منه بذلك.

Donna J. Abernathy, Online copyrights, Sep99, Vol. 53, Issue 9, Academic search premier.

(١) وهنا تبدو خصوصية الترخيص بالاستغلال في مجال البرامج المعلوماتية عن الترخيص بالنشر في المصنفات الأدبية والفنية الأخرى، حيث في الحالة الأخيرة يحصل المرخص له على حق إنتاج أي عدد من النسخ للمصنف(مع التزامه بالطبع والإعلان)، وذلك على عكس الحال بالنسبة للبرنامج، حيث لا يمنح المرخص له إلا استغلال النسخة الممنوحة له فقط. انظر د. **خالد مصطفى فهمي**، مرجع سابق، ص ٩١.

(٢) راجع سابقا، ص ٧٢ وما بعدها.

المعلوماتي من خلال البيع، أنه لا يملك في ظل هذه الحالة إلا أن يستعمل البرنامج استعمالاً شخصيًا، ولا يملك إعادة نسخه للغير[1]. غير أن هذا من شأنه أن يحد ويعطل من انتفاع البنك بالبرنامج على النحو الملائم لطبيعة نشاطه وأغراضه على شبكة الإنترنت؛ حيث إن انتفاع البنك بالبرنامج لا يتوقف عند الاستعمال الشخصي، بل يهم البنك أن يزود العميل بالبرامج التي تساعده على التواصل معه، من خلال إعادة نسخ هذه البرامج للعميل. ويدعم هذه الأهمية بالنسبة للبنك أمران:

(أ) طبيعة العمل المصرفي عبر شبكة الإنترنت تحتاج إلى سرعة في انجازها، ولن يتحقق ذلك إلا في ظل تسهيل إجراءات تواصل العميل مع البنك، من خلال اختصار البنك على العميل إجراءات البحث عن هذه البرامج وتزويده بها، خاصة إذا كانت هذه البرامج ذات مواصفات خاصة (متخصصة في المعاملات المصرفية)، قد يجد العميل صعوبة في الحصول عليها؛ مثل برنامج الدفع الإلكتروني (Electronic Payment)، وبرنامج الاطلاع على الحساب المصرفي (checking account balance)، وبرنامج إجراء التحويل الإلكتروني للنقود (Transferring funds)، وبرنامج دفع الفواتير (Paying bills)، وغيرها من البرامج اللازمة للتواصل مع البنك عبر شبكة الإنترنت[2].

---

(١) وقد عرفت المادة ١٣٨ قانون الملكية الفكرية المصري رقم ٨٢ لسنة ٢٠٠٢ **النسخ** بأنه عبارة عن " استحداث صورة أو أكثر مطابقة للأصل من مصنف أو تسجيل صوتي بأي طريقة أو في أي شكل بما في ذلك التخزين الإلكتروني الدائم أو الوقتي للمصنف أو التسجيل الصوتي".

(٢) وتشهد سوق البرامج المالية سباقا كبيرا من قبل كبرى شركات البرمجيات، حيث تسعى سعيا حثيثا لغزو فضاء المعاملات المصرفية عبر شبكة الانترنت، لتلبية حاجات عملائها من البنوك الإلكترونية العاملة عبر شبكة الانترنت، والتي تراقب هذا التسابق

(ب) يهم البنك أن يضمن استخدام العميل برامج موثوقًا بها، خاصة في ظل خطورة الجانب الأمني في نظام عمله، وفى ظل قلة خبرة العميل بتدارك هذا الأمر وحده[1]. ولن يتسنى للبنك تحقيق ذلك، إلا إذا حصل العميل على هذه البرامج بمعرفة البنك. ولن يتمكن البنك من ذلك إلا إذا تمتع بالحق في إعادة نسخها للغير[2].

وتأتى أهمية حصول البنك على الحق في إعادة نسخ البرنامج للغير في ظل تشدد النظم القانونية المختلفة في التأكيد على الحقوق الاستئثارية لمؤلف البرنامج، والتي تحظر على البنك إعادة نسخ البرنامج إلا إذا رخص له مؤلفه بذلك، وفى الحدود التي رخص له بها.

فقد نص قانون التجارة المصري ١٧ لسنة ١٩٩٩ في المادة (٨١) منه، على "لا يجوز للمستورد النزول للغير عن التكنولوجيا التي حصل عليها إلا بموافقة موردها". أيضا نص قانون الملكية الفكرية المصري رقم ٨٢ لسنة ٢٠٠٢ على هذه الحقوق في المادة (١٤٧) منه التي يجرى نصها على أن "يتمتع المؤلف وخلفه العام من بعده بحق استئثارى في الترخيص أو المنع لأي استغلال لمصنفه بأي وجه من الوجوه الخاصة وخاصة عن طريق النسخ أو البث الإذاعي أو

عن كثب سعيا للتواصل مع عملائها، من خلال تزويدهم بهذه البرامج التي تسهل عليهم التعامل مع البنك عبر شبكة الانترنت.

Dash, Julekha, Who'll get the lion's share of the electronic banking, Software magazine, March 1997, Vol. 17, Academic search complete, P. 18.

(1) **Shaoyi Liao- Yuan Pu Shao- Huaiqing Wang- Ada Chen**, Op. Cit., p. 69.

(2) **William Gram**; Op. Cit., p. 24.

الأداء العلني أو الترجمة أو التحوير أو التأجير أو الإعارة أو الإتاحة للجمهور، بما في ذلك إتاحته عبر أجهزة الحاسب الآلي أو من خلال شبكات الإنترنت أو شبكات المعلومات أو شبكات الاتصال أو غيرها من الوسائل".

أيضا نظم التوجيه الأوربي رقم (٩١/٢٥٠ EEC) الخاص بحماية برامج المعلومات على هذا الأمر، حيث نص على بعض الحقوق الاستئثارية (The exclusive rights)[١] لمؤلف البرنامج ومن يخوله ذلك، وهي:

١- نسخ البرنامج (Reproduction of a computer program).

٢- ترجمة وتعديل وترتيب البرنامج.

٣- توزيع البرنامج، بما يشتمل على ذلك من عائد مادي.

وقد نص على هذه الحقوق الاستئثارية أيضا قانون حماية الملكية الفكرية الإنجليزي، حيث منح مؤلف البرنامج كافة السلطات على مؤلفه، ومنحه أيضا الحق في رسم الإطار المناسب لمن يريد التمتع بإحدى هذه السلطات، وذلك من خلال الترخيص بالاستغلال التجاري لهذا المصنف على شبكة الإنترنت داخل الحدود المرسومة من قبل المؤلف[٢].

(١) ويقصد **بحق الاستئثار** أن المؤلف له حق احتكار واستغلال الانتاج الفكري بما يعود عليه من نفع مادي خلال مدة معينة طوال حياته وبعد مماته للخلف العام لمدة خمسين سنة وللمؤلف وحده هذا الحق، ولا يجوز مباشرته إلا بإذن من المؤلف إذا كان حيا أو إذنا من خلفه العام بعد الوفاة. انظر في ذلك د. **سعيد سعد عبد السلام**، الحماية القانونية لحق المؤلف والحقوق المجاورة، دار النهضة العربية، ٢٠٠٤، ص ١٠٧.

(2) **Stephen Rawson, Partner, Denton Wilde Sapte,** E-commerce-mobile transactions, Computer law & security report, Vol.18, no.3, 2002, p.166-167.

وفي الاتجاه ذاته نجد القانون الأمريكي الخاص بحماية المصنفات الرقمية (US Digital Millennium Copyright Act) الصادر عام ١٩٩٨[١]، حيث أعطى لمؤلف البرنامج الحق في وضع معايير تضمن له حماية مصنفه وحسن استخدامه، تحت أسم التدابير التقنية القياسية (Standard technical measures)، والتي تعرف بأنها عبارة عن مجموعة التدابير التي يضعها أصحاب الملكية الفكرية لتحديد وحماية أعمالهم. وقد اشترط هذا القانون أن تكون هذه المعايير موضوعية وعادلة ومعقولة ولا تتضمن شروطًا تمييزية، ولا تفرض تكاليف أو أعباء على مقدمي الخدمات الإلكترونية عند تعاملهم مع هذه البرامج أكثر مما ينبغي. كما فرض أيضا على مقدمي الخدمات الإلكترونية مراعاة هذه المعايير[٢].

---

(١) هذا القانون متاح على العنوان الإلكتروني النالى:

www.copyright.gov/legislation/dmca.pdf

(2) **Mark Turner and Mary Traynor, Herbert Smith,** UK E-commerce liability, Computer Law & Security Report, Vol. 19, no. 2, 2003, p. 117.

- هذا وقد قام المشرع الأمريكي بإصدار قانون لتعديل قانون حماية المصنفات الرقمية تحت أسم (copyright Term Extension Act of 1998 ("CTEA"). أراد من خلال هذا التعديل أن يوسع من الحماية المقررة لصاحب حق الملكية الفكرية، حيث وسع من مفهوم حماية الملكية الفكرية بأن جعله يمتد حتى ٧٠ عاما تالية لوفاة صاحب الحق بدلا من ٥٠ عاما، وفى الحالة التي يكون فيها حق الملكية الفكرية مقرر لأحد المؤسسات تتراوح المدة من ٧٥ إلى ٩٥ عاما، كما قرر أن تمتد هذه الحماية بصورة رجعية للأعمال السابقة على صدور القانون. وقد وجه لهذا القانون الكثير من الانتقادات، الكثير منها يتعلق بعدم دستوريته؛ نظرا لانه يشكل قيدا على حريات الإبداع والابتكار.

Stan J. Liebowitz&Stephen Margolis, Seventeen famous

وهذا ما أكده القضاء الأمريكي في أكثر من حكم[1]، حيث ذهب إلى أن المنتفع بالبرنامج المعلومات (البنك الإلكتروني) لا يمكنه استغلاله من خلال إعادة نسخه أو توزيعه إلا بعد أن يحصل على موافقة المؤلف بالاستغلال، وفى النطاق الذي رسمه له مؤلف البرنامج، بحيث يعد المنتفع متعديا متى استغل البرنامج بدون موافقة مؤلفه، أو خارج الحدود المسموح له فيها بالاستغلال.

ولعل هذا الحكم يعكس ما استقرت عليه التشريعات القانونية التي نظمت الحقوق الاستئثارية لمؤلف البرنامج؛ حيث لم تكتف بالتشديد على ضرورة الحصول على موافقة مؤلف البرنامج قبل استغلاله، بل ذهبت أيضا إلى التشديد على ضرورة الالتزام بالاستغلال في الإطار المحدد من قبل المؤلف، وإلا اعتبر المنتفع منتهكا لحقوق المؤلف، الأمر الذي يؤكد في النهاية ضرورة قيام البنك بالحصول على حق استغلال البرنامج من خلال إعادة نسخه من قبل مؤلفه.

نخلص من ذلك إلى أن البنك الإلكتروني، في ظل حاجته الماسة للحق في إعادة نسخ البرنامج، لن يكون أمامه سوى الحصول على ترخيص بذلك من مؤلفه.

---

economists weigh in on copyright: the role of theory, empirics, and network effects, Harvard journal of law & technology, Vol 18, N 2 Spring 2005, p 436

(1) **Court of Appeals for Federal Circuit**, Robert Jacobsen v. Matthew Katzer and Kamid associates, August 13, 2008. available at: www.mmmlaw.com

- **Venrnor v Autodesk**, inc, No.co7-1189 Raj(W.D.wash,sept.30,2009) available at:

http://jolt.law.harvard.edu/digest/category/software

٤٨- صور حصول البنك الإلكتروني على حق استغلال البرنامج:

يمكن أن يحصل البنك على حق استغلال البرنامج بإعادة نسخه من قبل مؤلفه، من خلال إحدى صورتين، على النحو التالي:

الصورة الأولى: إعداد البرنامج بناء على طلب البنك الإلكتروني:

يقوم البنك الإلكتروني في هذه الصورة بالتقدم لمؤلف برامج لإعداد برنامج معلوماتي ذي مواصفات خاصة، تلبى احتياجات البنك، وذلك نظير قيام البنك بدفع المقابل المناسب لذلك.

ويظهر هذا الفرض بصورة كبيرة في البرامج المتخصصة في المعاملات المصرفية، كبرنامج التحويل الإلكتروني للنقود، وبرنامج الدفع الإلكتروني وغيرها، حيث يحتاج إليها البنك بمواصفات معينة، فيلجأ إلى طلب تصميمها وفقا لهذه المواصفات.

هذا وقد سكت المشرع المصري عن تنظيم هذه الصورة من صور إعداد برامج المعلومات صراحة. لكن يمكن أن يستشف من نص المادة ١٥٢ من قانون الملكية الفكرية ٨٢ لسنة ٢٠٠٢ ما يفيد إمكانية قيام مؤلف البرنامج بإعداد برنامج خاص للبنك بناء على طلبه، حيث نصت هذه المادة على "ألا يترتب على تصرف المؤلف في النسخة الأصلية من مصنفه أيا كان نوع التصرف نقل حقوقه المالية. ومع ذلك لا يجوز إلزام المتصرف إليه بأن يمكن المؤلف من نسخ أو عرض النسخة الأصلية وذلك كله ما لم يتفق على غير ذلك". فعبارة "التصرف في النسخة الأصلية للبرنامج" يمكن أن توحي بأن هذه النسخة تم إعدادها بناء على طلب من حصل عليها، خاصة أن النص أعطاه الحق بألا يمكن

المؤلف من إمكانية نسخ أو عرض النسخة الأصلية بعد ذلك.

لكن التساؤل: هل يمتلك البنك الحق في استغلال البرنامج عن طريق إعادة نسخه في حالة إعداد البرنامج بناء على طلبه، حتى ولو لم يرد اتفاق صريح بين البنك ومؤلف البرنامج؟

ذهب جانب من الفقه[1] إلى أن إعداد البرنامج مادام قد تم بناء على طلب البنك، وقام بدفع تكلفته كاملة، فإن ذلك يعطيه الحق في إمكانية استغلاله من خلال إعادة نسخه حتى ولو لم يتم الاتفاق بينه وبين مؤلف البرنامج على ذلك.

ونحن من جانبنا لا نتفق مع هذا الرأي للأسباب التالية:

الأول: صياغة المادة ١٥٢ من قانون الملكية الفكرية ٨٢ لسنة ٢٠٠٢ سالفة الذكر، والتي لا تعطى لمن حصل على النسخة الأصلية (البنك) الحق في استغلال البرنامج عن طريق إعادة نسخه؛ حيث قرر هذا النص صراحة أن التصرف لا يترتب عليه نقل الحقوق المالية لمؤلف البرنامج.

الثاني: أن القول بأن إعداد البرنامج بناء على طلب البنك وقيامه بدفع تكلفته يعطيه الحق في إمكانية استغلاله عن طريق إعادة نسخه قول يعارض صريح النصوص السابقة (٨١ قانون التجارة، المادة ١٤٧، ١٥٢ من قانون الملكية الفكرية)[2]، والتي نهلت جميعها من معين واحد، وهو التأكيد والتشديد على

---

(١) د. **خالد مصطفى فهمي**، مرجع سابق، ص ٩٢.

(٢) نص **قانون التجارة المصري ١٧ لسنة ١٩٩٩** في المادة (٨١) منه على " لا يجوز للمستورد النزول للغير عن التكنولوجيا التي حصل عليها إلا بموافقة موردها".

- نص **قانون الملكية الفكرية المصري رقم ٨٢ لسنة ٢٠٠٢** في المادة (١٤٧) منه على " يتمتع المؤلف وخلفه العام من بعده بحق إستئثارى في الترخيص أو المنع لأي

الحقوق الاستئثارية لمؤلف البرنامج، دون أن تستثنى من ذلك حالة إعداد البرنامج بناء على طلب البنك.

الثالث: الترخيص بالاستغلال في مجال البرامج المعلوماتية يتمتع بخصوصية تميزه عن الترخيص بالنشر في المصنفات الأدبية والفنية الأخرى(١)، حيث في الحالة الأخيرة يحصل المرخص له على حق إنتاج أي عدد من النسخ للمصنف مع التزامه بالطبع والإعلان، وذلك على عكس الحال بالنسبة للبرنامج، حيث لا يمنح المرخص له إلا استغلال النسخة الممنوحة له فقط.

وبناءً عليه لن يبقى أمام البنك الإلكتروني في ظل أحكام القانون المصري إلا أن يحصل على ترخيص المؤلف صراحة في العقد المبرم بينهما بإعادة نسخه مرة أخرى.

وعن موقف التشريعات الأخرى في هذا الصدد، نجد أن المشرع الفرنسي قد نظم هذه الحالة، حيث أعطى للبنك الإلكتروني الحق في إعادة نسخ البرنامج حتى ولو لم يرد بذلك نص صريح في العقد المبرم بينه وبين ومؤلف البرنامج،

استغلال لمصنفه بأي وجه من الوجوه الخاصة وخاصة عن طريق النسخ أو البث الإذاعي أو الأداء العلني أو الترجمة أو التحوير أو التأجير أو الإعارة أو الإتاحة للجمهور، بما في ذلك إتاحته عبر أجهزة الحاسب الآلي أو من خلال شبكات الانترنت أو شبكات المعلومات أو شبكات الاتصال أو غيرها من الوسائل".

(١) ولعل هذا يعود كما يبرر القضاء الفرنسي إلى الطابع الابتكارى الذي يتميز به برنامج الكمبيوتر من احتوائه على وسيلة معالجة لمشكلة ما، وبأسلوب خاص يميز صاحبه، ويجعل من الصعب على الغير إعادة وصف البرنامج بذات الشكل والطريقة، للوصول إلى النتيجة التي توصل إليها المبرمج. كما أكد الفقه الفرنسي على ذات المعنى؛ حيث ذهب إلى أنه لا يمكن لاثنين متخصصين من الناحية الفنية أن يصلوا لهدف واحد باتباع نفس وسائل الشرح والعرض. د. **محمد عبد الظاهر حسين**، الاتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية، مرجع سابق، ص ٣٥

وذلك بشرط عدم وجود اتفاق يقضي بغير ذلك[1].

ومن الواضح أن المشرع الفرنسي قد تعامل مع هذه الحالة على أنها استثناء أراد من خلاله أن يعطى للمستخدم (البنك الإلكتروني) الحق في إعادة نسخ البرنامج، مادام البرنامج قد تم إعداده أصلا بناء على طلبه.

- الطبيعة القانونية لعلاقة البنك الإلكتروني بمؤلف البرنامج:

يتضح من خلال تدقيق النظر في تحديد طبيعة العلاقة بين البنك الإلكتروني ومؤلف البرنامج في هذه الحالة، أنها من قبيل عقود المقاولة [2]؛ حيث يلجأ البنك إلى أحد المتخصصين في أعمال البرمجة كي يقوم بتصميم برنامج بمواصفات معينة يحتاج إليها، وذلك نظير قيام البنك بدفع المقابل المالي لذلك، حيث ينطوي هذا الاتفاق على عناصر عقد المقاولة؛ من قيام المتخصص بعمل محدد وبصورة مستقلة (أي بدون خضوع لتوجيهات وإشراف البنك الإلكتروني)، نظير التزام البنك بدفع المقابل المالي المتفق عليه. ومن ثم يسرى على هذا الاتفاق القواعد العامة في القانون المدني المصري الخاصة بعقد المقاولة[3].

لكن يجب ملاحظة أن تكييف العلاقة بين البنك ومؤلف البرنامج في هذا الفرض على أنها عقد مقاولة لا تخل بتمتع المؤلف على البرنامج بحقوقه الأدبية،

(١) د. **خالد مصطفى فهمي**، مرجع سابق، ص ٩٢.

(٢) د. **محمد حسين منصور**، مرجع سابق، ص ٣٨.

(٣) وقد عرفت المادة ٦٤٦ من القانون المدني المصري عقد المقاولة بأنه " عقد يتعهد بمقتضاه أحد المتعاقدين أن يصنع شيئا أو يؤدى عملا لقاء أجر يتعهد به المتعاقد الآخر". وعرف أيضا بأنه "عقد يقصد به أن يقوم شخص بعمل معين لحساب شخص آخر في مقابل أجر، ودون أن يخضع لإشرافه أو إدارته" انظر د. **محمد لبيب شنب**، أحكام عقد المقاولة، منشأة المعارف، الطبعة الثانية، ٢٠٠٤، ص ١٩.

والتي من أهمها نسبة البرنامج له.

الصورة الثانية: حصول البنك على ترخيص بنسخ البرنامج:

في هذه الصورة يكون هناك برنامج سابق التجهيز، أعده مؤلفه للتداول، وهذا عادة ما يكون بالنسبة للبرامج النمطية، مثل (برامج معالجة النصوص، وبرامج إجراء العمليات الحسابية)[١]، ويحتاج البنك الإلكتروني إلي إستعماله وإعادة نسخه للعملاء، هنا يلجأ البنك إلى مؤلف البرنامج، ويطلب منه الترخيص له بإعادة نسخه مرة أخرى، وذلك نظير مقابل (أجر) يراعى فيه نطاق هذا الترخيص من ناحية الكم، والمدة الزمنية لذلك.

وقد نظم المشرع المصري هذه الحالة في المادة ١٤٧ من قانون الملكية الفكرية سابق الذكر، حيث أعطى لمؤلف البرنامج حقًا استئثاريًا في الترخيص باستغلال مصنفه، عن طريق النسخ، بهدف نقل العمل للجمهور بصورة مباشرة أو غير مباشرة، وذلك بموجب عقد يبرم مع مؤلف البرنامج، يصرح فيه بذلك[٢].

- الطبيعة القانونية لعلاقة البنك الإلكتروني بمؤلف البرنامج

تكيف العلاقة بين البنك الإلكتروني ومؤلف البرنامج في هذه الحالة على أنها من قبيل عقود الترخيص[٣]، والتي يمنح بموجبها صاحب الحق على شيء معين

---

(١) د. **محمد عبد الظاهر حسين**، مرجع السابق، ص٧١.

(٢) د. **خالد مصطفى فهمي**، مرجع سابق، ص ٩٢.

(٣) د. **السيد محمد السيد عمران**، الطبيعة القانونية لعقود المعلومات، مؤسسة الثقافة الجامعية، ١٩٩٢، ص ٧٦؛

Michael D. Scott, Liability in cyberspace – III, Computer law & secu-

بعض السلطات التي يملكها على هذا الشيء، لشخص ما، وذلك وفقا لإطار معين يحدده له صاحب هذا الحق.

هذا ولا يوجد نص في النظام القانوني المصري يعرف عقد الترخيص.

وقد عرف هذا العقد في القانون الأمريكي الموحد لنقل وتبادل المعلومات (UCITA) بأنه عبارة عن "عقد يخول فيه المرخص للمرخص له سلطات الاستعمال والتوزيع وإعادة الإنتاج للمعلومات أو الحقوق المعلوماتية التي يملكها، وذلك وفقا للحدود التي يسمح بها المرخص"(١).

وعرف أيضا(٢) بأنه: "العقد الذي بمقتضاه يضع أحد الطرفين (المرخص) تحت تصرف الطرف الآخر (المرخص له) براءة اختراع أو معرفة فنية معينة، بهدف استغلالها في مجال إنتاجي معين، وذلك خلال مدة معينة، وفقا لشروط محددة، لقاء مقابل مالي".

واستنادا لهذا العقد، يحصل البنك الإلكتروني على الحق في الانتفاع بالبرنامج، عن طريق استعماله، أو استغلاله (إعادة نسخه)، وذلك نظير التزام

---

rity report, Vol. 13, no. 6, 1997, 452. **Donna J. Abernathy**, Online copyrights, Op, Cit.: -**HSBC**, Internet banking, terms and conditions, available at: http://www. bahrain.hsbc.com/public/ mere-gional/bahrain_hom/pOpups/en/bah_pib_terms.jhtml

(1) **Uniform computer information transaction ACT**, on uniform state laws, annual conference, Colorado, July 23-30, 1999, part one. Available at: www.law.upenn.edu/ bll/archiues/ulc/uCita/2002final.pdf.

(٢) انس السيد عطية سليمان، الضمانات القانونية لنقل التكنولوجيا إلى الدول النامية والمشروعات التابعة لها، رسالة دكتوراه، كلية الحقوق- جامعة عين شمس، ١٩٩٦، ص٢٩٢.

البنك بدفع مقابل ذلك. ويحدد العقد بطبيعة الحال إطار الانتفاع بالبرنامج من خلال تحديد مدة الانتفاع، والنطاق الجغرافي لذلك.

لكن يثور تساؤل في هذا الصدد، هل يعد عقد الترخيص بانتفاع البنك بالبرنامج على هذا النحو من قبيل عقود نقل التكنولوجيا؟

يرى جانب من الفقه[١] أن عقد الترخيص في هذه الحالة لا يعد من قبيل عقود نقل التكنولوجيا[٢]، وقد أصل هذا الجانب رأيه بالقول بأن عقد الترخيص في هذا الفرض موضوعه ليس نقل التكنولوجيا من خلال استعمالها كقيمة، وإنما فقط تنظيم الحقوق الواردة على هذه التكنولوجيا بوصفها قيمة مبادلة، بمعنى آخر العقد يمنح البنك الحق في استغلال البرنامج من خلال إعادة نسخه للعملاء فقط، في ظل تمتع المؤلف بكافة حقوقه عليه، ولا يعطي البنك الحق في اكتساب البرنامج. ويؤكد على هذا بالقول بأن نقل التكنولوجيا ليس موضوعا لهذا العقد، وحتى إن حدثت بعض مظاهر لهذا النقل، فما هذا سوى أثر من آثار العقد وليس موضوعه الأساسي.

ونحن من جانبنا نتفق مع هذا الرأي فيما ذهب إليه. ونضيف تأكيدًا لهذا الموقف أن كلمة نقل الواردة في عبارة نقل التكنولوجيا لا يقف معناها عند حد تسليم البرنامج للبنك مع إحاطته علما بكيفية تشغيله وإعادة نسخه. فكلمة النقل

---

(١) المرجع السابق، ص ٢٩٥.

(٢) يقصد بكلمة تكنولوجيا، (مجموعة الدراسات والبحوث والمعارف التي تهدف إلى انتقاء وتجسيد نتائج الاكتشافات والبحوث العلمية ــ القابلة للتطبيق العملي ــ في شكل آلات،أو أجهزة، أو طرق صناعية جديدة، أو تطبيقات جديدة في مجال الأنشطة الاقتصادية، صناعية كانت أو زراعية أو تجارية أو خدمية). **د.محمود مختار أحمد بريرى**، إبرام عقود نقل التقنية وتحديد محلها، مجلة الأمن والقانون، كلية شرطة دبي، السنة الرابعة،العدد الأول، ١٤١٦- ١٩٩٦، ص٣٠٢.

ذات دلالة أبعد من ذلك، حيث إنها تمتد لتشمل السيطرة الكاملة على البرنامج أي نقل الحق في البراءة ذاتها، بما يترتب على ذلك من ضرورة تزويد المتلقي بكافة الجوانب الخفية في نظام اختراع البرنامج بما يتيحه ذلك من إمكانيـة تطـويره والاستفادة منه، وهذا ليس موضوع العقد بين مؤلف البرنامج والبنك الإلكتروني. فالأخير يسعى فقط للحصول على حق استعمال البرنامج، وإمكانية إعادة نسخه للعملاء.

وأيا ما كانت الصورة التي تظهر عليها علاقـة البنـك الإلكترونـي بمؤلـف البرنامج (ترخيص، مقاولة)، فإن من أهم الالتزامات التي تقع على عاتق مؤلف البرنامج، هو تسليم البرنامج وفقا للمواصفات المتفق عليها في العقد المبرم بينه وبين البنك، وأن يراعى في التسليم ذات الاعتبارات المقررة على عاتق مـورد المكونات المادية لشبكة البنك، والتي سبق تفصيلها(١).

٣)- التزامات البنك الإلكتروني في مواجهة مؤلف البرنامج:

٤٩- تتعدد الالتزامات الواقعة على عاتق البنك بموجب العقد الذي يحكم علاقته بمؤلف البرنامج، ومعظم هذه الالتزامات تقليدية (كالالتزام بدفع مقابل اسـتغلال البرنامج)، لكن ما نود تسليط الضوء عليه، في ضوء أهميته هو الالتزام بسرية البرنامج.

ويقصد بالالتزام بسرية البرنامج التزام البنك بالحفاظ على سرية المعلومـات والبيانات التي يتكون منها البرنامج من الاطـلاع عليهـا، أو بالتعـديل فيهـا

---

(١) انظر سابقا، ص ٧٣.

بالتحريف أو التغيير[1].

فالتزام البنك الإلكتروني بالسرية بهذا المعنى هو بمثابة الحصن الحصين لمؤلف البرنامج، الذي يضمن له عدم الاطلاع على المعلومات الخاصة بتكوين البرنامج، ومن ثم تجنب استغلالها بدون موافقته، أو الاعتداء على البرنامج بالتحريف أو التبديل.

ويثور التساؤل عن نطاق هذا الالتزام في علاقة مؤلف البرنامج بالبنك الإلكتروني؟

يمكن الإجابة على هذا التساؤل بأن البنك يجب عليه أن يضمن لمؤلف البرنامج سريته داخل نطاق استفادة البنك بهذا البرنامج؛ بمعنى أن يلتزم البنك بضمان تحقيق هذا الالتزام من قبله شخصيا ومن قبل كل من يتعاملون مع البرنامج بمعرفة البنك، سواء من العاملين لدى البنك، أم من عملائه الذين يحصلون على نسخة من هذا البرنامج.

ويثور التساؤل هنا عن حكم خلو العقد المبرم بين البنك الإلكتروني ومؤلف البرنامج من النص صراحة على الالتزام بالسرية؟

لا يوجد في النظام القانوني المصري نص صريح يعالج المحافظة على سرية البرنامج من قبل المرخص له باستعماله، لكن هذا لا يمنع من القول بإثقال كاهل البنك بهذا الالتزام، وذلك لسببين:

الأول/ إذا كان المشرع المصري قد نظم الالتزام بالسرية في قانون التجارة ١٧

([1]) **Chris Reed&John Angel**; Op. Cit, p. 461.

لسنة ١٩٩٩ بخصوص عقد نقل التكنولوجيا[1]، ذلك العقد الذي يمنح المستورد للتكنولوجيا سلطات أوسع على التكنولوجيا المنقولة إليه من تلك التي يتيحها عقد الترخيص للبنك الإلكتروني باستغلال البرنامج، فمن باب أولى يكون البنك ملتزما بسرية البرنامج في ظل تمتعه بسلطات أقل عليه.

الثاني/ أن الالتزام بالسرية في خصوص الترخيص باستغلال البرنامج من مقتضيات هذا العقد وفقا لطبيعة محله، ووفقا للمستقر عليه في قواعد العرف والعدالة في هذا الخصوص؛ فالبرنامج عبارة عن مجموعة معلومات ذات طابع ابتكاري مصوغة في شكل معين من قبل مؤلفها، الأمر الذي يقتضى اعتبارها من قبيل الأسرار حتى ولو لم يرد نص صريح في العقد يفيد ذلك.

ويعد التزام البنك بالمحافظة على سرية البرنامج وفقا لطبيعته ولسلطات البنك عليه التزامًا بتحقيق نتيجة، بمعنى أن البنك ملتزم بالامتناع عن الاطلاع على البيانات الخاصة بالبرنامج أو تحريفها بأى شكل، ولا يكتفي منه أن يبذل عناية في ذلك.

وأخيرا يظل الالتزام بالسرية مثقلا لكاهل البنك الإلكتروني حتى بعد انتهاء العقد المبرم بينه وبين مؤلف البرنامج لأي سبب (انتهاء مدته، أو فسخ العقد)[2]،

---

(١) حيث نص في المادة (٨٣) فقرة (١) من هذا القانون على أن "يلتزم المستورد بالمحافظة على سرية التكنولوجيا التي حصل عليها وعلى سرية التحسينات التي تدخل عليها، ويسأل عن تعويض الضرر الذي ينشأ عن إفشاء هذه السرية سواء وقع في مرحلة التفاوض على إبرام العقد أو بعد ذلك" كما أضاف في الفقرة الثانية من ذات المادة " يلتزم المورد بالمحافظة على سرية التحسينات التي يدخلها المستورد وينقلها بموجب شرط في العقد، ويسأل المورد عن تعويض الضرر الذي ينشأ عن إفشاء هذه السرية.

(٢) وهذا ما أكدت عليه المذكرة الإيضاحية لقانون التجارة الجديد رقم ١٧ لسنة ١٩٩٩،

بحيث إذا قام البنك باستغلال البرنامج على الرغم من ذلك، يمكن لمؤلف البرنامج أن يعود عليه بدعوى المنافسة غير المشروعة وفقا لأحكام المادة (١٦٣ من القانون المدني المصري)(١).

هذا وقد نظم قانون التجارة الإنجليزي صراحة على الالتزام بالسرية في خصوص عقد استغلال البرامج المعلوماتية، حيث اعتبر أن هذه البرامج من قبيل الأسرار التجارية التي يتعين الالتزام صراحة أو ضمنا بسريتها (Implied or express obligation of confidence)(٢).

وقد أعتبر قانون الأسرار التجارية الموحد في الولايات المتحدة الأمريكية (The Uniform Trade Secrets Act) أيضا البرنامج المعلوماتي من قبيل الأسرار التجارية التي يجب المحافظة عليها من قبيل المرخص له باستعماله(٣).

وبناء عليه نهيب بالمشرع المصري لكي يتدخل لتوفير حماية قانونية أكبر لبرامج المعلومات، وذلك بالنص الصريح على اعتبارها من قبيل الأسرار التجارية التي يجب المحافظة عليه من قبل مستعمل البرنامج، وذلك لسببين:

حيث جاء فيها " يلزم المستورد بالمحافظة على سرية التكنولوجيا التي يحصل عليها، بما يترتب على ذلك من مسؤولية عن تعويض الضرر الذي يترتب على إفشائه لهذه السرية، ويبرز هذا الالتزام بالسرية على عاتق المستورد ابتداءً من لحظة دخوله في مفاوضات مع المورد لإبرام عقد نقل التكنولوجيا، ويبقى الالتزام قائما على عاتقه حتى ولو فشلت المفاوضات ولم يتم إبرام العقد"

(١) د. **محمد عبد الظاهر حسين**، المرجع السابق، ص٧٥، راجع أيضا د.**خالد مصطفى فهمي**، مرجع سابق، ص ١٥٦

(2) **Michael chissick, Alistair Kelman**,; Op. Cit., p. 161.

(3) **William Gram**,; Op. Cit., p 24

الأول: أن اعتبار البرنامج من قبيل السر التجاري، سيجعل البنك والعاملين لديه والمتعاملين معه من قبيل الأمناء على هذا السر[1]، ومن ثم تزداد وتشدد مسؤوليتهم القانونية في المحافظة عليه.

الثاني: الأهمية الكبرى التي تتمتع بها هذه البرامج في عصر ثورة المعلومات، حيث أضحت برامج المعلومات هي مصدر الثروة ومحركها. ولعل هذه الخصوصية تزداد بخصوص البرامج الخاصة بالمعاملات المصرفية الإلكترونية، والتي تحتل أهمية خاصة في ضوء ما تحتاجه هذه المعاملات من برامج ذات مواصفات خاصة تتناسب مع طبيعة المعاملات المصرفية من دقة وتنظيم وتأمين. لذلك يجب على المشرع أن يولى مزيدا من الأهمية لهذه البرامج، حتى يشجع مؤلفي هذه البرامج على طرحها وتطويرها، وحتى يشجع البنك على إعادة طرحها للعملاء وهو يطمئن إلى التزامهم بالمحافظة على سرية البرنامج.

٤) مسؤوليات الأطراف المتعاقدة:

بعد التعرض لالتزامات كل من مؤلف البرنامج المعلوماتي والبنك، يثور التساؤل حول طبيعة مسؤولية كل منهما تجاه الأخر في ضوء الالتزامات السابقة، وذلك على النحو التالي:

أولا: مسؤولية مؤلف البرنامج:

يستدعى الحديث عن مسؤولية مؤلف البرنامج، التعرض لهذه المسؤولية في

(١) د.**أشرف توفيق شمس الدين**، الحماية الجنائية للمستند الإلكترونى، الدليل الإلكتروني للقانون العربى، (بدون تاريخ نشر)، ص ٣٠، متاح على العنوان الإلكتروني التالى: www.arablawinfo.com

مواجهة البنك، وفى مواجهة العملاء، وذلك على النحو التالي:

أ- مسؤولية مؤلف البرنامج في مواجهة البنك الإلكتروني:

٥٠- يمكن أن تثور مسؤولية مؤلف البرنامج في مواجهة البنك الإلكتروني في عدة حالات على النحو التالي:

- المسؤولية العقدية، فأيا ما كانت صورة العقد التي تحكم العلاقة بين البنك ومؤلف البرنامج(عقد ترخيص أو عقد مقاولة)، فهو مسئول في مواجهة البنك الإلكتروني كقاعدة عامة عن تحقيق نتيجة معينة؛ هي تسليم البنك برنامجًا صالحًا للاستعمال وفق احتياجاته، (هذا بطبيعة الحال ما لم يكن هناك اتفاق على غير ذلك)، ومن ثم تتعقد مسؤوليته العقدية في حالة عدم تحقق النتيجة المتفق عليها. ويكفى البنك في ذلك إثبات عدم تحقق النتيجة حتى تنعقد مسؤولية المؤلف، ولا يستطيع الأخير دفعها إلا بإثبات السبب الأجنبي(١).
- المسؤولية التقصيرية، ويسأل مؤلف البرنامج عن كل خطأ ناجم عن البرنامج- خارج نطاق العقد- تسبب في إلحاق الضرر بالبنك الإلكتروني. ويجب على البنك الإلكتروني أن يثبت خطأ المؤلف الذي تسبب في الإضرار به، وذلك طبقا للقواعد العامة المنصوص عليها في المادة (١٦٣) من القانون المدني المصري.

- المسؤولية الموضوعية. يمكن أن يسأل مؤلف البرنامج أيضا على أساس نظرية المخاطر، وذلك في حالة أن لحق بالبنك الإلكتروني ضرر نتيجة استعماله للبرنامج، حتى ولو لم يصدر خطأ من جانب مؤلف البرنامج (عقدي أو

---

(١) د. **أحمد شوقي عبد الرحمن**، مرجع سابق، ص ٢٠٣.

تقصيري)، وذلك وفقا لما سبق ذكره بخصوص مسؤولية بائع الأجهزة في مواجهة البنك الإلكتروني[1].

ب- مسؤولية مؤلف البرنامج في مواجهة عملاء البنك الإلكتروني:

٥١- لا يسأل مؤلف البرنامج عقديا في مواجهة عملاء البنك، حيث لا يوجد بينهما عقد يبرر قيام هذه المسؤولية. بيد أنه يمكن لهم الرجوع على مؤلف البرنامج طبقا لقواعد المسؤولية التقصيرية، إذا لحقهم ضرر نتيجة خطأ صدر عن مؤلف البرنامج، كما يمكن لهم الرجوع على المؤلف أيضا بموجب قواعد المسؤولية الموضوعية، تلك التي تقضى بمسؤولية مؤلف البرنامج عن الأضرار الناتجة عن نشاطه، حتى ولو لم يرقى هذا النشاط لدرجة الخطأ باعتبار أن نشاط مؤلف البرنامج ينطوي على مخاطر قد تلحق بالمستفيدين بهذا البرنامج، ومن ثم يسأل عن هذه المخاطر.

ثانيًا: مسؤولية البنك الإلكتروني في مواجهة مؤلف البرنامج:

٥٢- يشكل الحديث عن مسؤولية البنك الإلكتروني تجاه مؤلف البرنامج أهمية خاصة، هذه الأهمية تنطلق من طبيعة استعمال البنك للبرنامج، وطبيعة الالتزامات المفروضة عليه بموجب العقد الذي يحكم علاقته بمؤلف هذا البرنامج. فالبنك ليس مجرد مستخدم عادى لهذا البرنامج، ولكنه يستعمل أحد الحقوق الاستئثارية المملوكة للمؤلف، من خلال إمكانية إعادة نسخ هذا البرنامج لعملائه. يضاف إلى ذلك الالتزامات المفروضة عليه في مواجهة مؤلف البرنامج، والتي يأتي في مقدمتها المحافظة على سرية هذا البرنامج، واستغلاله

---

(١) راجع سابقا، ص ٨٧.

في الإطار المرسوم له من قبل مؤلفه، الأمر الذي يقتضى التعرض لمسؤولية البنك في مواجهة مؤلف البرنامج على النحو التالي:

(١) المسؤولية الجنائية للبنك فى مواجهة مؤلف البرنامج:

٥٣- يسأل البنك الإلكتروني جنائيا عن الاعتداءات التي تقع على البرنامج المعلوماتى[١] وفقا لنص المادة ١٨١ من قانون الملكية الفكرية المصري، والتي تنص على أنه "مع عدم الإخلال بأي عقوبة أشد في قانون آخر يعاقب بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن خمسة ألاف جنيه ولا تزيد على عشرة آلاف جنيه، أو بإحدى هاتين العقوبتين، كل من أرتكب أحد الأفعال الآتية:

- بيع أو تسجيل مصنف أو تسجيل صوتي أو برنامج إذاعي محمى طبقا لأحكام هذا القانون أو طرحه للتداول بأي صورة بدون إذن كتابي مسبق من المؤلف أو صاحب الحق المجاور.
- تقليد مصنف أو تسجيل صوتي أو برنامج إذاعي أو بيعه أو طرحه للتداول أو للإيجار مع العلم بتقليده.
- التقليد في الداخل لمصنف أو تسجيل صوتي أو برنامج إذاعي أو أداء محمى طبقا لأحكام هذا القانون عبر أجهزة الحاسب الآلي أو شبكات الإنترنت أو

---

(١) ويأتي حرص التشريعات المختلفة على توفير الحماية الجنائية لبرامج المعلومات بصورة عامة من الأهمية الاقتصادية الكبيرة لهذه البرامج، والتي تعد بحق من الركائز المحورية التي تدور حولها عولمة الاقتصاد الرقمي، لذا فقد أخذت العديد من التشريعات على عاتقها مهمة توفير الحماية الجنائية لهذه البرامج وذلك لمواجهة أشكال الاعتداء المختلفة عليها. انظر

Katyal, Neal Kumar, Criminal law in cyberspace, Academic Search Premier, Apr2001, Vol. 149, Issue 4, p 34.

شبكات المعلومات أو شبكات الاتصالات أو غيرها من الوسائل بـدون إذن كتابي مسبق من المؤلف أو صاحب الحق المجاور.

- التصنيع أو التجميع أو الاستيراد بغرض البيـع أو التـأجير لأي جهـاز أو وسيلة أو أداة مصممة أو معدة للتحايل على حماية تقنية يستخدمها المؤلف أو صاحب الحق المجاور كالتشفير أو غيره.

- الاعتداء على أي حق أدبي أو مالي من حقوق المؤلف أو الحقوق المجاورة المنصوص عليها في هذا القانون".

وبما أن المشرع المصري في قانون ٨٢ لسنة ٢٠٠٢ (واتفاقية التريبس من قبله)، قد اعتبر أن البرامج المعلوماتية من قبيل المصنفات الأدبية التـي تحمـى بقوانين حق المؤلف[١]، فأن النص العقابي سالف الذكر يحمى مؤلف البرنامج في مواجهة كل من يأتي أحد الأفعال السابقة. ويترتب على ذلـك أن يـسأل البنـك الإلكتروني جنائيا في حالة أن أتى أحد الأفعال التي عددها النص العقابي السابق، هذا بالإضافة إلى بعض العقوبات التكميلية التي نصت عليها المادة (١٨١ سالفة الذكر)، وهي إمكانية قيام المحكمة بمصادرة النسخ محل الجريمة أو المتحـصلة منها، وكذلك المعدات والأدوات المستخدمة في ارتكابها، ويجوز للمحكمة كـذلك أن تغلق المنشأة التي تم استغلالها في ارتكاب الجريمة مدة لا تزيد علـى سـتة أشهر.

وقد تعاملت المادة ٤١٨ من قانون العقوبات الفرنسي مع صور الاعتـداء

(١) تنص **المادة ١٤٠ من القانون رقم ٨٢ لسنة ٢٠٠٢** بإصدار قانون حماية الملكيـة الفكرية على " تتمتع بحماية هذا القانون حقوق المؤلفين على مصنفاتهم الأدبية والفنية وبوجه خاص المصنفات الآتية... (٢) برامج الحاسب الآلي.

على البرنامج تحت وصف جريمة إذاعة أو نشر الأسرار الصناعية (Secret de abrique). وقد نصت هذه المادة على معاقبة الجاني بالسجن من سنتين لخمس سنوات أو الغرامة التي لا تقل عن ١٨٠٠ يورو ولا تزيد على مائة وعشرين ألف يورو، وذلك إذا تمت إذاعة هذه الأسرار داخل فرنسا. أما إذا أذيعت خارج فرنسا، فالعقوبة الحبس من ثلاثة شهور إلى سنتين والغرامة التي لا تقل عن خمسمائة يورو، ولا تزيد عن ثمانمائة يورو[١].

هذا وقد تعاملت المحكمة العليا في بريطانيا **(High Court)** مع الانتهاك الواقع من قبل البنك على البرنامج المعلوماتي الذي يستعمله بصورة مشددة، تمثلت في اعتبار هذا الاعتداء مشكلاً لجريمتين مستقلتين، الأولى هي الاعتداء على حق مؤلف البرنامج، والثانية خيانة الثقة (**separate claim for breach of confidence**)[٢].

وهذا الاتجاه من قبل هذه المحكمة يعكس حرصا على حماية مؤلف البرنامج، ويفترض أنه عندما يسمح لأحد الأشخاص باستعمال البرنامج الخاص به، فإنه يمنحه ثقة في عدم الاعتداء على الحقوق الخاصة به على البرنامج.

ولعل هذا يدعونا إلى توجيه النداء للمشرع المصري بضرورة إفراد نص خاص بحماية سرية برامج المعلومات، وذلك بالنظر إلى تمتعها بخصوصية في مواجهة سائر المصنفات الأدبية والفنية الأخرى، خاصة في مثل حالة البنك الإلكتروني، الذي يحصل على ترخيص من المؤلف بإعادة نسخه، الأمر الذي

---

(١) **د. خالد مصطفى فهمي**، مرجع سابق، ص ١٧١.

(2) **Nigel Miller**, UK E-commerce Bill -- Progress?, computer fraud & security, November 1999, p 12

يعكس ثقة كبيرة من قبل المؤلف عند الترخيص للبنك بذلك، ومن ثم يجب أن تشدد العقوبة إذا ما أخل البنك بهذه الثقة واعتدى على البرنامج.

(٢) المسؤولية المدنية للبنك فى مواجهة مؤلف البرنامج:

٥٤- من الممكن أن تثور المسؤولية المدنية للبنك الإلكتروني في مواجهة مؤلف البرنامج في الحالات التالية:

- المسؤولية العقدية؛ وذلك في حالة إخلال البنك الإلكتروني بأحد الالتزامات العقدية؛ كإفشاء سرية البرنامج. ويكفى مؤلف البرنامج في هذه الحالة إثبات وجود التزام البنك (العقد الذي يحكم علاقته بالبنك)، حتى تنعقد مسؤوليته، دون الحاجة لإثبات خطأ البنك في هذا الخصوص، حيث أنه ملتزم بتحقيق نتيجة (المحافظة على سرية البرنامج)[1]، ومن ثم لن يستطيع البنك الإلكتروني أن يدفع مسؤوليته في هذه الحالة إلا بإثبات السبب الأجنبي. أيضا تنعقد المسؤولية العقدية للبنك الإلكتروني في حالة حدوث الإخلال من قبل أحد العاملين لدى البنك، أو عملائه، مادام البنك متعهدا في العقد المبرم بينه وبين مؤلف البرنامج بالتزام العاملين لديه بهذا الالتزام (كما لو تعهد البنك بالمحافظة على سرية البرنامج من قبل من يتعاملون مع البرنامج بمعرفة البنك).

- المسؤولية التقصيرية؛ حيث يسأل البنك الإلكتروني مدنيا في مواجهة مؤلف البرنامج في حالة ارتكابه خطأ (غير عقدي) سبب ضررا لمؤلف البرنامج، يستوي في ذلك أن يشكل هذا الخطأ جريمة وفقا لقانون العقوبات، أو لا

(١) د.**محمد عبد الظاهر حسين**، مرجع سابق، ص٢.

يصل إلى حد الجريمة؛ كما لو كان يشكل عملا من أعمال المنافسة غير المشروعة.

- مسؤولية المتبوع عن فعل التابع، حيث يسأل البنك الإلكتروني مدنيا في حالة وقوع الخطأ من جانب أحد العاملين لدى البنك، مما أوقع الضرر بمؤلف البرنامج، وذلك بموجب قواعد مسؤولية المتبوع عن أعمال تابعيه(١). فمادام قد وقع خطأ من أحد العاملين لدى البنك أثناء قيامه بمهام وظيفته أو بسببها، وكان يرتبط بالبنك بعلاقة تبعية (١٧٤ مدني مصري) تنشأ مسؤولية البنك المدنية. وفي هذه الحالة يملك المؤلف الرجوع على العامل مباشرة، أو الرجوع عليه وعلى البنك متضامنين. وفي كافة الأحوال يجوز للبنك الإلكتروني الرجوع على هذا العامل بما أداه من تعويض(٢).

وقد اعترف القضاء الأمريكي صراحة بمسؤولية رب العمل (البنك الإلكتروني) عن الانتهاكات التي تقع من قبل العاملين لديه على الأشياء المحمية بقوانين الملكية الفكرية. وقد اشترط لقيام هذه المسؤولية شرطين(٣):

الأول: إذا كان رب العمل (البنك الإلكتروني) يعلم، أو كان يجب عليه أن يعلم وفقا للسير الطبيعي للأمور بالانتهاكات التي يقوم بها العاملين لديه.

الثاني: ألا يقوم– على الرغم من هذا العلم– باتخاذ الإجراءات المناسبة لمنع هذه

---

(1) **Michael D. Scott**; Op. Cit., p. 452.

(٢) ويبرر ذلك من قبل غالبية الفقه بأن مسؤولية المتبوع عن فعل التابع تقوم على فكرة الضمان، ومن ثم يستطيع المضرور من فعل التابع الرجوع على المتبوع، وإمكانية رجوع الأخير على التابع بما أداه من تعويض. د. **أحمد شوقي عبد الرحمن**، مرجع سابق، ص ٣٢٧.

(3) **Michael D. Scott**; Op. Cit., p. 452.

الأنشطة (took no steps to curb those activities).

ويبدو أن القضاء الأمريكي بهذه الشروط قد أراد أن يخفف من مسؤولية البنك الإلكتروني بخصوص الانتهاكات التي يمكن أن تقع من قبل العاملين لديه على حقوق مؤلف البرنامج، حيث إنه لم ينتهج ذات النهج الذي سار عليه المشرع المصري- والذي افترض الخطأ في جانب البنك الإلكتروني لمجرد وجود علاقة تبعية تجمع البنك بالعاملين لديه- بل اشترط لتحقق خطأ البنك ومن ثم قيام مسؤوليته، علمه الفعلي، أو وجوب علمه وفقا للسير الطبيعي للأمور بالانتهاكات التي تقع من قبل العاملين لديه، واتخاذ البنك موقفا سلبيا حيال ذلك. ويبدو أن القضاء الأمريكي قد لمس روح العدالة في هذا النهج؛ حيث إنه لم يستبعد مسؤولية البنك عن هذه الانتهاكات تماما (رعاية لمصالح مؤلف البرنامج)، وفي ذات الوقت لم يطلق العنان لقيام هذه المسؤولية لمجرد وجود علاقة تبعية (رعاية لمصالح البنك الإلكتروني)، بل اشترط إضافة لهذه التبعية علم البنك بالخطأ الواقع من أحد العاملين لديه، وسكوته على ذلك رغم هذا العلم. فإذا كان الحرص على حقوق المؤلف تدفعنا لتشديد المسؤولية، فأن الحرص ذاته يجذبنا إلى توفير مناخ قانوني متزن للبنوك الإلكترونية العاملة عبر شبكة الإنترنت. كل ذلك يجعلنا نهيب بالمشرع المصري إلى ضرورة التدخل لصياغة قواعد خاصة بمسؤولية البنوك الإلكترونية العاملة عبر شبكة الإنترنت عن العاملين لديها، كي تلائم طبيعة عمل هذه البنوك وتلائم البيئة التي تحيا فيها.

ثالثا- مسؤولية العاملين لدى البنك الإلكتروني:

٥٥- يمكن إقامة مسؤولية العاملين لدى البنك الإلكتروني في فروض عدة:

- يسأل العامل لدى البنك الإلكتروني جنائيا بموجب نص المادة ١٨١ من قانون الملكية الفكرية المصري سالف الذكر، وذلك في حالة ارتكابه أي فعل من شأنه أن يشكل اعتداء على حق مؤلف البرنامج؛ وذلك كما لو قام دون أن يحصل على إذن من المؤلف بنسخ البرامج المحملة على أجهزة البنك، أو ببيعها، أو تأجيرها، أو تقليدها مع علمه وإرادته. ويستوي قيامه بهذه الأعمال أثناء عمله لدى البنك الإلكتروني أو بعد انتهاء هذا العمل.

- يسأل العامل لدى البنك الإلكتروني مدنيا (على أساس المسؤولية التقصيرية) في مواجهة مؤلف البرنامج، وذلك في حالة ارتكابه خطأ- يستوي أن يكون هذا الخطأ مشكلاً لجريمة، أو لا يصل إلى هذا الحد- سبب ضررا لمؤلف البرنامج (حسبما تقضى المادة ١٦٣ من القانون المدني المصري). ويجب على مؤلف البرنامج في هذه الحالة إثبات خطأ هذا العامل حتى تنعقد مسؤوليته.

- كما يمكن أن تثور مسؤولية العامل مدنيا في مواجهة البنك الإلكتروني، إذا شكل خطأ العامل في حق مؤلف البرنامج، إخلالا بأحد الالتزامات الواردة في عقد العمل الذي يحكم علاقة البنك الإلكتروني بالعامل. ومن أمثلة هذا الخطأ أن يشترط البنك الإلكتروني على العامل المحافظة على سرية البرنامج (وهو التزام بتحقيق نتيجة)، ويخل العامل بهذا الالتزام. ويكفي في هذه الحالة أن يثبت البنك عدم تحقق النتيجة المرجوة من الالتزام دون أن يثبت خطأ هذا العامل؛ حتى تقوم مسؤولية الأخير.

وأخيرا يثور التساؤل حول مدى مسؤولية عميل البنك عما يصدر عنه من أخطاء بخصوص استعماله للبرامج المسلمة له من البنك؟

٥٦- مضت الإشارة إلى أن البنك الإلكتروني غالبا ما يلجأ إلى تزويد عملائه ببعض البرامج التي يحتاجون إليها للتعامل مع البنك عبر شبكة الإنترنت، وعادة ما يحرص البنك على هذا الأمر، وذلك كخدمة يقدمها البنك لعملائه، خاصة أن معظم هذه البرامج ليست برامج نمطية، بل تكون برامج متخصصة قد يصعب على العميل الحصول عليها من مكان آخر(كبرامج الدفع الإلكتروني للنقود)، وحتى يضمن البنك تعامل العميل معه ببرامج جيدة تتمتع بدرجة عالية من الثقة والأمان. لذلك يمكن أن تثور مسؤولية هذا العميل عن أخطائه التي تقع أثناء استخدامه هذا البرنامج على النحو التالي.

- تنشأ المسؤولية الجنائية للعميل في حالة قيامه بنسخ البرامج التي في حيازته ثم قيامه ببيعها، أو تأجيرها، أو تقليدها، مع علمه وإرادته، وذلك وفقا للمادة ١٨١ من قانون الملكية الفكرية سالفة الذكر.
- تنشأ المسؤولية المدنية للعميل في حالة ارتكابه خطأ سبب ضررا لمؤلف البرنامج، سواء وصل هذا الخطأ إلى حد الجريمة أم لم يصل. ويسأل العميل مدنيا على أساس المسؤولية العقدية في مواجهة البنك الإلكتروني وذلك إذا أخل بواجب المحافظة على البرامج التي حصل عليها من البنك، وكان ملتزما بالمحافظة عليها.
- تنعقد المسؤولية المدنية التقصيرية في مواجهة مؤلف البرنامج، وذلك في حالة ارتكابه خطأ سبب ضررًا لمؤلف البرنامج، وهو بصدد استعماله للبرنامج.

المبحث الثاني

عقود الخدمات الإلكترونية اللازمة لتواجد البنك الإلكتروني على شبكة الإنترنت

٥٧- تتعدد وتتنوع عقود الخدمات الإلكترونية على شبكة الإنترنت بصورة عامة، بل أن هذا التعدد في زيادة مستمرة؛ نظرا لوجود رغبة ملحة، مصحوبة بنزعة تنافسية في غزو البيئة الافتراضية من قبل قطاعات الأعمال المختلفة، الأمر الذي ألقى على عاتق مقدمي الخدمات الالكترونية بمهمة تمهيد وتهيئة التعامل مع هذه البيئة الوعرة، من خلال الخدمات التي يقدمونها لحسن الاستفادة من مقدراتها. وقد عظم ذلك من دور مقدمي الخدمات الالكترونية، وجعلهم يحتلون مكانة كبرى؛ بالنظر إلى دورهم المحوري في تسيير حركة التعامل على شبكة الإنترنت بصورة عامة.

وقد تحلى دور مقدمي الخدمات الالكترونية بثوب الخصوصية في نظام البنك على شبكة الإنترنت[1]؛ فالطبيعة الخاصة للنشاط المصرفي تتطلب حرصا زائدا على استمرارية تقديم الخدمة وسهولة الحصول عليها، يضاف لذلك خطورة عامل الأمن في نظام عمل البنك، والذي قد يتهدد بسبب احتمالية اطلاع مقدمي الخدمات الإلكترونية- أثناء قيامهم بأعمالهم- على بعض البيانات المصرفية. وقد دعت هذه الخصوصية إلى ضرورة إيجاد تنظيم قانوني يحكم وينظم علاقتهم بالبنك، من خلال التعرض لأهم الالتزامات المتبادلة، وطبيعة المسؤولية الناشئة

---

(1) **E-Banking,** Federal Financial Institutions Examination Council; Op. Cit., p. 3.

عنها، وذلك في ظل الطبيعة الخاصة للنشاط المصرفي، وللبيئة الإلكترونية (شبكة الإنترنت).

وبناء عليه، فسوف نتناول فقط أهم العقود اللازمة لتواجد البنك وتشغيله على شبكة الإنترنت، والتي تستجمع أهم الالتزامات القانونية التي يمكن أن يلتزم بها مقدمو الخدمات الإلكترونية في مواجهة البنك والعكس، وهى عقد الدخول على الانترنت، وعقد تصميم الموقع الإلكتروني للبنك، وعقد الإيواء، وذلك على النحو التالي:

المطلب الأول

عقد دخول البنك لشبكة الإنترنت

٥٨- يأتي عقد الاتصال أو الدخول لشبكة الإنترنت في مقدمة عقود الخدمات الإلكترونية اللازمة لتواجد البنك على شبكة الإنترنت، حيث تعد الخدمة محل هذا العقد بمثابة حلقة الوصل بين البنك وهذه الشبكة، والخطوة الأولى نحو تواجده عليها(١).

وتحتل خدمة الدخول (محل هذا العقد) أهمية خاصة بالنسبة للبنك؛ تبررها أمران:

- ارتباط وجود البنك وتشغيله بالاتصال بالإنترنت، حيث إن حاجة البنك للإنترنت لا تتوقف عند مجرد الإعلان عن خدماته (كما هو الحال بالنسبة لمعظم المؤسسات المتصلة بالإنترنت)، بل أن الأمر يمتد ليشمل

---

(1) **G C Chalikias**; Op. Cit, p. 2

التعاقد مع العملاء، وتنفيذ الخدمة المصرفية المطلوبة من خلال الاتصال بالإنترنت.

- عدم قدرة البنك على الإحاطة بنفسه بالجوانب الفنية للتعامل مع الأجهزة والبرامج الخاصة بالاتصال بالإنترنت.

والأمر على هذا النحو يربط حسن اتصال البنك وتواصله مع عملائه عبر شبكة الإنترنت بحسن تقديم خدمة الدخول للبنك. لذلك تبدو أهمية بيانِ ماهيةِ عقد دخول البنك لشبكة الإنترنت، وتفصيل أهم الالتزامات التي يرتبها على عاتق أطرافه، والمسؤوليات الناشئة عن الإخلال بهذه الالتزامات، وذلك على النحو التالي:

أولا: ماهية عقد دخول البنك لشبكة الإنترنت:

٥٩- يعرف عقد الدخول لشبكة الإنترنت بأنه عبارة عن اتفاق يلتزم بمقتضاه مقدم خدمة الدخول بتمكين البنك الإلكتروني من الاتصال فنيا بشبكة الإنترنت[١]، وذلك نظير التزام البنك بدفع المقابل المالي المتفق عليه[٢].

---

(١) ويقصد بالاتصال فنيا بشبكة الانترنت توفير كافة الوسائل التقنية التي تمكن البنك من الاتصال بشبكة الانترنت، والتي من أهمها برنامج الاتصال، والذى يعمل على تحقيق الربط بين شبكة البنك الداخلية وشبكة الانترنت، بالإضافة لبعض الإجراءات اللازمة لتسجيل الموقع الإلكتروني للبنك لدى الجهات المختصة.

(٢) د. **سمير حامد الجمال**، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، الطبعة الأولى، ٢٠٠٦، ص٧٩؛ د. **محمد حسين منصور**، مرجع سابق، ص ٢٦؛ د. **خالد ممدوح إبراهيم**، إبرام العقد الإلكتروني، دار الفكر الجامعي، ٢٠٠٦؛ ص ٧٣؛ د.**إيمان مأمون سليمان**، الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، ٢٠٠٦، ص ٦٥.

ويتضح من خلال هذا التعريف أمران:

الأول/ أن عقد الدخول لشبكة الإنترنت من العقود المستحدثة في نشاط البنـوك، فرضته مقتضيات التعامل على شبكة الإنترنت، الأمر الذي يقتضي تأثر التزامات ومسؤوليات مقدم الخدمة بخصوصيات النشاط المصرفي.

الثاني/ أن عقد دخول البنك لشبكة الإنترنت عقد ملزم للجانبين، يتسم فيه التـزام مقدم الخدمة بالطابع الفني، من خلال تحقيق نتيجة محددة؛ وهى اتصال البنـك بشبكة الإنترنت، وذلك نظير التزام البنك بدفع المقابل المالي.

ويعرف مقدم خدمة الدخول (Internet service provider)[١] كطرف مناظر للبنك الالكتروني؛ بأنه عبارة عن " شخص طبيعي أو معنوي يعمل على ربـط البنك بشبكة الإنترنت، بالإضافة لتقديم بعض الخدمات الأخرى المرتبطة بهـذا الدخول، مثل تسجيل العنـوان الإلكترونـي (Domain name registration) البنك"[٢].

---

(١) **يطلق على مزود الخدمة** أسماء كثيرة منها متعهد الوصول أو متعهد الخدمة أو مقـدم الخدمة. ويتصف عمل مزود الخدمة بأنه ذو طبيعة فنية، فهو الذي يمكن مـستخدمي الانترنت من الوصول إلى المواقع الإلكترونية أو البريد الإلكتروني للأشخاص الـذين يريدون مخاطبتهم. وبمعنى أوضح يتمثل دور مزود الخدمة فـي ربـط مـستخدمي الانترنت بالشبكة عن طريق عقود اشتراك تؤمن لهم هـذه الخدمـة. ومـن أشـهر الـشركات العاملـة فـي هـذا المجـال شـركة **CompuServe**، وشـركة **DemonInternet**، وشركة **Microsoft**، وشركة **Pipex**، وشركة**AOL**. انظر **د. شريف محمد غنام**، التنظيم القانوني للإعلانات التجارية عبر شبكة الانترنت، بدون دار نشر، ٢٠٠٦، ص٨: ١٠.

Julian JB Hickey – Robin Mathew-ChristOpher; Op., Cit, p. 15.

(2)**Internet service provider**, Wikipedia, free encyelopedia, available at: http://en.wikipedia.org/wiki/Internet_service_provider; **B. Nor-**

ويلاحظ من خلال هذا التعريف أن مقدم خدمة الدخول يتعاقد مع البنك على أداء عمل ذي طبيعة فنية، وبصورة مستقلة، بعيدا عن تدخل البنك؛ بمعنى أن الأخير لا يملك سلطة إصدار تعليمات أو توجيهات لمقدم خدمة الدخول من الناحية الفنية، الأمر الذي يفهم منه أن مقدم خدمة الدخول لا يرتبط بالبنك بعقد عمل، ولكن التكييف الذي يغلب على هذه العلاقة كما يذهب جانب من الفقه(1)- بحق- أنها عقد مقاولة، يلتزم فيها مقدم الخدمة بالقيام بعمل تظير أجر.

هذا وقد تغافل القانون المصري للتوقيع الإلكتروني ١٥ لسنة ٢٠٠٤ وباقي القوانين العربية المعنية بالتجارة الإلكترونية(2) عن وضع تنظيم قانوني خاص بمقدمي الخدمات الإلكترونية على شبكة الإنترنت- وذلك باستثناء بعض الأحكام الخاصة بمقدمي خدمات التوثيق الإلكتروني- سواء من ناحية تنظيم شروط عملهم، أو الالتزامات الواقعة عليهم، أو المسؤولية المترتبة على إخلالهم

---

ton, Internet service providers and peering, IN" 2..1, P. 1 available at: http://www.equinix.com/pdf/ whitepapers/PeeringWP.2.pdf

- عرف أيضا بأنه عبارة عن شركة تقوم ببيع خدمة الدخول لشبكة الانترنت (sells access to the internet)، للبنك، وغيرها من خدمات الانترنت الأخرى.

Michael chissick, Alistair Kelman, Op. Cit., p. xxxix

(١) **د. محمد حسين منصور**، مرجع سابق، ص٣٤.

(٢) القانون التونسي الخاص بالمبادلات والتجارية الإلكترونية قانون عدد ٨٣ لسنة ٢٠٠٠، متاح على العنوان الإلكتروني التالي: http://www.arabegov.com/News/News.asp?id=5914، القانون الأردني (قانون المعاملات الإلكترونية) رقم ٨٥ لسنة ٢٠٠١، متاح على العنوان الإلكتروني التالي: www.ecipit.org.eg/Arabic/pdf/Ardon_low.pdf، القانون الإماراتي "قانون المعاملات والتجارة الإلكترونية" رقم (٢) لسنة٢٠٠٢، متاح على العنوان الإلكتروني التالي: www.ecipit.org.eg/Arabic/pdf/Dubi_low.pdf، القانون المصري (قانون التوقيع الإلكتروني وهيئة تنمية تكنولوجيا صناعة المعلومات) ١٥ لسنة ٢٠٠٤. انظر الجريدة الرسمية العدد ١٧ تابع (د) في ٢٢ أبريل ٢٠٠٤.

بمسؤولياتهم.

ويبدو لنا أن هذا الوضع منتقد. فالدور المحوري الذي يقوم به مقدم خدمة الدخول في خدمة التجارة الإلكترونية بصورة عامة، والبنك الإلكتروني على الإنترنت بصورة خاصة، يجعلنا نهيب بالقائمين على سلطة التشريع في هذه الدول بضرورة التدخل لتنظيم عمل هؤلاء خاصة من يتصدى منهم لتقديم الخدمات للبنك على الإنترنت، وذلك من خلال اشتراط توافر مؤهلات أو خبرات معينة لديهم، وكذلك وضع إجراءات رقابية على عملهم، تضمن التزامهم بأداء مهامهم، وأيضا تنظيم بعض الالتزامات القانونية التي يجب عليهم مراعاتها، ومسؤوليتهم عن تنفيذ هذه الالتزامات في مواجهة البنك.

ولم يظهر لنا في هذا الصدد، إلا مشروع قانون الإنترنت والمعلوماتية الفلسطيني(١)، والذي صاغ بعض النصوص لتنظيم شروط حصول مقدم الخدمة على ترخيص لمزاولة عمله، حيث نص في المادة الأولى فقرة (هـ) على وجوب حصول مقدم خدمات الإنترنت على ترخيص لتقديم هذه الخدمة. وقد عرف هذا الترخيص بأنه عبارة عن "إجازة تصدرها الوزارة تسمح لشخص بتقديم خدمة الإنترنت وغيرها من خدمات القيمة المضافة".

كما تعرض هذا المشروع في المادة (٩) لشروط حصول مقدم خدمة الدخول على الإنترنت على ترخيص وهي:

- أن يكون طالب الرخصة مسجلا ضمن قوائم التأهيل المعدة من قبل

---

(١) هذا القانون متاح على العنوان الإلكتروني التالي:
http://www.pita-palestine.org/PITA%2 files/proposed%2.e-commerce%2.law.doc

الوزارة، وتتوافر فيه الإمكانات الفنية والإدارية والمالية لتقديم الخدمة المطلوبة رخصتها.

- أن يكون الطالب مسجلا في السجل التجاري أو سجل الشركات حسب مقتضى الحال تسجيلا ساري المفعول، وطوال فترة الترخيص، وحاصلاً على أية تراخيص لازمة لمزاولة نشاطه مع جهات أخرى.
- على طالب الرخصة أن يقدم ما يفيد موافقة الجهة الرسمية المختصة على أنشطته الإضافية لخدمة الإنترنت والمعلوماتية.
- تقديم كفالة بنكية تحدد قيمتها بموجب اللوائح والتعليمات التي تصدرها الوزارة.

ويحمد لواضعي هذا المشروع صنيعهم؛ حيث إنهم استخدموا عبارات مناسبة للشروط الواجب توافرها في مقدم خدمة الدخول من شأنها أن تراعي توافر متطلبات خاصة فيمن يقدم خدمة الدخول للبنك. فعبارة "وتتوافر فيه الإمكانات الفنية والإدارية والمالية لتقديم الخدمة المطلوبة رخصتها" وعبارة "وحاصلاً على أية تراخيص لازمة لمزاولة نشاطه مع جهات أخرى"، من شأنها أن تفيد أن الشروط المطلوبة ليست موحدة، بل تختلف بحسب طبيعة نشاط المؤسسة طالبة الخدمة، الأمر الذي يفيد ضرورة أن يكون مقدم خدمة الدخول للبنك على دراية بطبيعة الخدمات المصرفية، ومن ثم تأتي خدماته ملاءمة لطبيعة نشاط البنك.

وعلى الصعيد الدولي نجد أن قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية (١٩٩٦) جاء خاليا من تنظيم قانوني خاص بمقدمي خدمات الإنترنت من حيث تنظيم حقوقهم والتزاماتهم القانونية، حيث أنشغل هذا القانون بتنظيم

العلاقة القانونية بين منشئي رسائل البيانات والمرسل إليهم، وغفل عن مقـدمي خدمات الإنترنت على الرغم من الدور البالغ الأهمية لهم في تيـسير التجـارة الإلكترونية(١).

أيضا جاء التوجيه الأوربي رقم ٣١/٢٠٠٠ في المادة الخامسة(٢) منه، يلـزم مقدمي الخدمات الإلكترونية عند تقديم خدماتهم، أن يقدموا لطالبي الخدمة (البنك الإلكتروني) كافة البيانات الخاصة بهم، والتي تفيد في التعرف عليهم، مثل بيان بالرخصة التي تؤهله لتقديم الخدمات الإلكترونية، والطريقة التي سيتم من خلالها التعاقد، وكل بنود وشروط العقد الذي سيحكم تقديم الخدمة. وأضاف إلى ذلك أن مقدم الخدمة يجب عليه أن يمكن طالب الخدمة من الاطلاع على كل هذه البيانات والاحتفاظ بها(٣).

وعلى ما يبدو فإن التوجيه الأوربي نأى بنفسه عن وضع تنظـيم قـانوني يحكم وينظم التزاماتِ ومسؤوليات مقدمي الخدمة بشكل تفصيلي (هذا وأن كـان هناك بعض التوجيهات القليلة التي نظمت بعض الأمور الخاصة بمقدمي الخدمة بصورة عامة كما سيأتي الحديث عنها فيما بعد) وأحال في خصوص ذلك إلـى العقود التي ستحكم عملهم(٤). ولعله أراد من وراء هذا تفعيل مبدأ سلطان الإرادة

---

(١) **قانون الاونيسترال النموذجي بشأن التجارة الإلكترونية**، منشورات الأمـم المتحـدة، ٢٠٠٠، ص ٢٨

Available at: http://w.unCitral.org

2) **Directive 2000/31/EC**, Official journal of the european communities, 8 June 2000.

(3) **Stephen Rawson, Partner, Denton Wilde Spate**; Op. Cit., p. 164.

(4) **Directive EC,** Official journal of the european communities,2000/31.

في هذه الخدمات المستحدثة، وترك المجال متسعا أمام هؤلاء الوافدين الجدد لتنظيم التزاماتهم ومسؤولياتهم بما يساعدهم على تقديم خدماتهم، وحتى لا تكون كثرة النصوص القانونية وكثرة ما تحمله من التزامات ومسؤوليات عبئا ثقيلا عليهم في هذه المرحلة.

لكن الأمر في النهاية يعكس حالة من الفراغ التشريعي لدى العديد من الدول فيما يتعلق بتنظيم عقد الدخول على شبكة الإنترنت، وما ينبثق عنه من التزامات ومسؤوليات تقع على مقدمي خدمة الدخول، خاصة في ضوء طبيعة النشاط المصرفي. أيضا غياب تنظيم قانوني لالتزامات ومسؤولية البنك الإلكتروني في مواجهتهم. لذا فأننا سنحاول حصر هذه الالتزامات، وتنظيم هذه المسؤوليات، من خلال ترسم خطى القضاء تارة، واستقراء عقود الخدمات الإلكترونية تارة أخرى، وذلك على النحو التالي:

ثانيًا- التزامات مقدم خدمة الدخول والبنك الإلكتروني:

٦٠- ذكرنا فيما سبق أن العلاقة بين البنك الإلكتروني ومقدم خدمة الدخول يحكمها عقد الدخول لشبكة الإنترنت، وهو عقد تبادلي؛ يفرض التزامات متبادلة على عاتق طرفيه، وذلك على النحو التالي:

(١) التزامات مقدم خدمة الدخول تجاه البنك الإلكتروني:

٦١- تتعدد الالتزامات الواقعة على عاتق مقدم خدمة الدخول تجاه البنك الإلكتروني. ونعرض في هذا المقام لأهم هذه الالتزامات المتصور أنها تمثل الحد الأدنى لما يجب أن تكون عليه علاقة البنك بمقدم خدمة الدخول، وذلك على التفصيل التالي:

- انطلاقا من الطابع الفني لنشاط مقدم خدمة الدخول، يأتي في مقدمة الالتزامات التي يلتزم بها تجاه البنك، تزويده بكافة الأجهزة والبرامج والموصلات اللازمة للاتصال بشبكة الإنترنت. ويجب أن يحرص مقدم الخدمة على أن يقدم أفضل أنواع هذه الأجهزة والبرامج، على نحو يتلاءم مع طبيعة عمل البنك وحجم نشاطه، حيث تتوقف سرعة اتصال البنك بشبكة الإنترنت، وتواصله مع العملاء من خلالها على نوع الأجهزة والبرامج التي يعتمد عليها **البنك** في الاتصال[١]. وتختلف هذه الأجهزة بحسب الطريقة التي يختار البنك الاتصال من خلالها بشبكة الإنترنت. فقد يتم هذا الاتصال عن طريق خط تليفوني، حيث يحتاج البنك في هذه الحالة إلى مودم (Modem)[٢]، بالإضافة إلى خط تليفوني عادي أو يتم الاتصال عن طريق خط (ISDN)[٣]، وهو خط اتصال يعمل على ربط أجهزة البنك بشبكة

---

(1) **Chris Reed**; Op. Cit., P. 91.

(٢) وهو عبارة عن جهاز إلكتروني يعمل على تحويل الرموز الرقمية (Digital Signals) المندفعة من خط التليفون إلى إشارات تناظرية (Analog Signals) يستطيع الحاسب فهمها. ويمكن أن يكون هذا الجهاز مثبتًا داخل الحاسب المراد توصيله بالانترنت (Internal Modem)، أو يكون منفصلا عنه (Eternal Modem). **د. نشأت الخميسي**، مرجع سابق، ص ٨٦.

(٣) وهو اختصار يشير إلى شبكة الخطوط الرقمية المجمعة (Integrated Services Digital Network)، حيث تعمل هذه الشبكة على زيادة سرعة نقل البيانات عبر شبكة الانترنت، أو عبر شبكة اتصال محلية عن بعد، خاصة إذا ما تعلق الأمر بملفات ذات حجم كبير مثل الصوت والصورة وهو اختصار يشير إلى شبكة الخطوط الرقمية المجمعة (Integrated Services Digital Network)، حيث تعمل هذه الشبكة على زيادة سرعة نقل البيانات عبر شبكة الانترنت، أو عبر شبكة اتصال محلية عن بعد، خاصة إذا ما تعلق الأمر بملفات ذات حجم كبير مثل الصوت والصورة. وتصل السرعة في الشبكات المحلية منها إلى ١٢٨ بايت في الثانية، كما يمكن تزيد هذه السرعة في حالة وجود خطوط تجارية (Commercial Link).

الخطوط الرقمية المجمعة الخاصة بمقدم خدمة الدخول، بحيث يصبح البنك أحد أعضاء هذه الشبكة المجمعة والمتصلة بشبكة الإنترنت(1). وغالبا ما يلجأ البنك الإلكتروني إلى الطريقة الثانية نظرا لما توفره من سرعة كبيرة في الاتصال بشبكة الإنترنت، بالإضافة إلى أنها أقل من حيث التكلفة المادية. لكن يؤخذ على هذه الطريقة أنها تمكن الأعضاء من التواصل فيما بينهم، من خلال دخول أي منهم على البيانات الموجودة على أجهزة الآخر (Sharing Information) (٢). لذلك يجب على البنك أن يغطي هذه الخاصية، وذلك لاعتبارات تتعلق بسرية البيانات المحملة على أجهزته، ويجب ملاحظة أن التزام مقدم خدمة الدخول لا ينتهي عند حد تسليم هذه الأجهزة والبرامج للبنك، بل يجب أن يقوم بتحقيق اتصال البنك بشبكة الإنترنت بالفعل(٣)؛ وذلك من خلال تمكين البنك من الدخول إلى شبكة الإنترنت عن طريق الأجهزة الخاصة به.

- تزويد البنك الإلكتروني بكافة النصائح(٤)، والإرشادات التي تبين له كيفية

---

(1) **Julian JB Hickey – Robin Mathew-ChristOpher**;Op .Cit, p. 13; **Steffen Lippert, Giancarlo Spagnolo,** Internet peering as network of relations, Telecommunications policy, February 2008, Vol 32, Issue 1, p. 33-49.

(2) **Julian JB Hickey – Robin Mathew-ChristOpher**; Op. Cit, p14.

(3) **G C Chalikias**; Op. Cit, p. 2
د. سمير حامد الجمال، مرجع سابق، ص٧٩؛ **د. محمد حسين منصور**، مرجع سابق، ص ٢٦

(٤) وقد ذهبت محكمة باريس في أحكامها الصادرة في ٦ مارس ١٩٨١، ٤ يونيو ١٩٨٠. إلى أن واجب النصيحة يقع على عاتق كل مقدم للأجهزة الإلكترونية، وأن هذا الالتزام يمكن أن يظهر في صور عديدة، كصرف المستخدم عن استخدام أحد الأنظمة، أو تقييم احتياجات المستخدم، وتقديم الحلول المناسبة له بحسب احتياجاته.

استعمال الأجهزة والبرامج التي قدمها له للدخول إلى شبكة الإنترنت، مثل كيفية تشغيل برنامج الاتصال (بما في ذلك أفضل الأرقام التي سيقوم البنك باستعمالها للدخول على شبكة الإنترنت وذلك إذا كان الاتصال يتم عن طريق التليفون)، أو اسم المستخدم ID وكلمة المرور Password (إذا كان الاتصال يتم عن طريق خط ISDN). ويجب على مقدم الخدمة أن يتابع ويشرف على طريقة استعمال البنك لهذه الأجهزة والبرامج[1].

ويحتل هذا الالتزام بهذا المعنى أهمية خاصة بالنسبة للبنك؛ تبررها أهمية خدمة الدخول بالنسبة للبنك، والتي يعتمد عليها البنك للإعلان والتعاقد وتنفيذ خدماته المصرفية عليها، الأمر الذي يفرض ضرورة إحاطة البنك علما بكيفية التعامل مع أجهزة وبرامج الاتصال بالإنترنت. يأتي ذلك في ظل عدم علم البنك بهذه الجوانب.

وفى ظل هذه الأهمية، يغيب عن القانون المصري نص خاص يلزم مقدم الخدمة بإعلام البنك. لكن القواعد العامة يمكن أن تستوعب هذا الفرض؛ وذلك باعتبار أن التزام مقدم الخدمة بإعلام البنك بكافة الجوانب الفنية المتعلقة بالاتصال بشبكة الإنترنت من مقتضيات العقد وفقا لطبيعة المحل والغرض من التعاقد (المادة ١٤٨ من القانون المدني المصري). لكن هذا الأمر على هذا

- C A Pairs 5e ch 4 Janv, 1981.
- C A Pairs 5e ch, 6 mars 1981.

مشار إلى هذه الأحكام لدى د. نبيلة إسماعيل رسلان، مرجع سابق، ص ١٨.

(١) د. حسن حسين البراوى، عقد تقديم المشورة، دار النهضة العربية، ١٩٩٨، ص ٢٦٧؛ انظر أيضا د. محمد عبد الظاهر حسين، المسؤولية القانونية في مجال شبكات الانترنت، دار النهضة العربية، ١٤٢٢-٢٠٠٢، ص ٧٤.

النحو لا يكفى من وجهة نظرنا، حيث يجب على المشرع أن يتدخل بنص صريح يعالج من خلاله التزام مقدم خدمة الدخول بإعلام البنك بالجوانب الفنية للاستفادة من الخدمة، نظرا لأهمية هذا الالتزام بالنسبة للبنك، الذي غالبا ما يجهل هذه الأمور الفنية.

وعلى صعيد التشريعات الأخرى، فالملاحظ أنها أولت اهتماما لهذا الالتزام؛ حيث أوصى التوجيه الأوربي (EC/2000/31) بضرورة التزام مقدم الخدمة بتزويد البنك الإلكتروني بكافة البيانات والإرشادات الخاصة بعملية التعاقد، وكيفية الحصول على الخدمة محل العقد، وذلك على النحو الذي يجعل البنك في حالة إلمام بكافة التفاصيل الخاصة بهذه الخدمة(١).

وفى ذات السياق، فقد أوصى المجلس الوطني للاستهلاك في فرنسا- في تقرير حديث له- ببعض الالتزامات التي يجب أن يراعيها مقدم خدمة الدخول، لتحسين مستوى الخدمة والوصول بها إلى الصورة المثلى، أهمها:

- أن يعلم مقدم الخدمة البنك الإلكتروني بمدى كفاءة الخطوط المستعملة وعدد المشتركين لديه، وذلك حتى يكون البنك على بينة بمدى كفاءة أدوات الاتصال بالعملاء.

- أن يعلم البنك الإلكتروني بالبرامج المتوافرة لديه ومدى حداثتها، وأن يقدم له البرامج اللازمة للتوافق بين خدمات الشبكة وبين الأجهزة التي يستخدمها(٢).

---

(1) **Stephen Rawson, Partner, Denton Wilde Sapte,** Op. Cit., p 164

(٢) **د. فريد عبد المعز فرج،** التعاقد بالانترنت، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون – فرع دمنهور، العدد الثامن عشر، الجزء الأول ١٤٢٤هـ – ٢٠٠٣

أيضا أوصى المجلس الوطني بدولة الإمارات العربية في خصوص مشروع عقد الاشتراك في الإنترنت ببعض المقترحات، والتي يقف ورائها رغبة المجلس في توفير أكبر قدر ممكن من الشفافية في مواجهة متلقي الخدمة، من خلال تزويده بأكبر قدر ممكن من عناصر التوضيح والإعلام. لذلك أوصى المجلس بضرورة التزام مقدم الخدمة بتزويد البنك الإلكتروني بما يلي[١]:

- كافة البيانات المتعلقة ببرامج التشغيل.
- تقديم وصف تفصيلي لطبيعة وكيفية تشغيل الخدمة المقدمة، وطرق متابعتها.
- كيفية تخزين وإدارة الرسائل الإلكترونية.

والأصل في التزام مقدم الخدمة بتقديم النصائح والإرشادات للبنك أنه التزام ببذل عناية، بحيث يتحقق التزام مقدم الخدمة ببذل العناية المناسبة لإحاطة البنك الإلكتروني علما بكافة جوانب تشغيل الأجهزة والبرامج، حتى ولو لم يتحقق هذا الإعلام بالفعل.

وكما سبق أن ذكرنا[٢] معيار بذل العناية (Duty of Care) كوسيلة لقياس الالتزام قد شهد تطورا كبيرا في معاملات التجارة عبر شبكة الإنترنت، حيث أصبح يقاس في ضوء طبيعة المخاطر المرتبطة بنشاط الملتزم، بما يفرض عليه تفهم طبيعة هذه المخاطر وبذل عناية تتناسب معها، وذلك بمعيار المحترف في

م، ص٤٩٨.

(١) د. عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الانترنت، دار الفكر الجامعي، الطبعة الأولى، ٢٠٠٦، ص٧٧.

(٢) أنظر سابقا، ص ٨١.

أعمال الكمبيوتر والشبكات.

وبناء عليه يجب ألا يقتصر بذل العناية من قبل مقدم الخدمة في مواجهة البنك على مجرد ترديد إرشادات وتعليمات نصية وحسب، بل يجب عليه أن يبذل كل جهده لإحاطة البنك علما بكافة التفاصيل الخاصة بالتعامل مع الأجهزة والبرامج، مع تقديم الشرح والتدريب الكافي لذلك.

- يلتزم مقدم خدمة الدخول تجاه البنك الإلكتروني بتقديم خدمة المساعدة الفنية، والتي يطلق عليها خدمة الخط الساخن (Hot line) [١]، حيث تحل العديد من المشاكل الفنية المتعلقة بدخول البنك على شبكة الإنترنت عن طريق هذه الخدمة، من خلال التليفون. ويمثل هذا الالتزام أهمية كبرى في علاقة البنك بمقدم خدمة الدخول؛ حيث من المتصور أن يواجه البنك أعطالا فنية في أحد الأجهزة أو البرامج الخاصة بعملية الاتصال بالإنترنت، وذلك على النحو الذي يفقد معه البنك شريان التواصل مع عملائه، ومن ثم يجب أن يلتزم مقدم خدمة الدخول بالتصدي لمثل هذه الأمور، من خلال تقديم الإصلاحات الفنية اللازمة لذلك.

وخدمة الخط الساخن يمكن أن تدخل في إطار العقد (عقد الدخول لشبكة الإنترنت) باعتبارها عنصرا رئيسيا في هذا العقد[٢]، أو ينظمها عقد خاص بها[٣].

وأيا ما كانت الصورة التي سيتم من خلالها تنظيم هذه الخدمة، هناك بعض

---

(١) د. **سمير حامد الجمال**، مرجع سابق، ص٨٦

(٢) د. **خالد ممدوح إبراهيم**، مرجع سابق، ص ٧٣

(٣) د. **ايمان مأمون أحمد سليمان**، مرجع سابق، ص ٦٧

الالتزامات الواقعة على عاتق مقدم خدمة الدخول بمناسبة هذه الخدمة، وهي[1]:

- أن يحدد للبنك الوقت الذي يجوز له طلب خدمة الخط الساخن والوقت المحدد للرد عليه.
- تحديد خدمات المساعدة الفنية التي يلتزم بتقديمها، وتلك التي تخرج عن نطاق اختصاصه.
- تحديد متوسط المدة القصوى المخصصة لحل المشاكل التي يطرحها البنك الإلكتروني.

(٢) التزامات البنك الإلكتروني تجاه مقدم خدمة الدخول:

٦٢- يلتزم البنك الإلكتروني في مواجهة مقدم خدمة الدخول بموجب عقد الدخول إلى شبكة الإنترنت بمجموعة من الالتزامات، وذلك على النحو التالي:

أ) يلتزم البنك بدفع المقابل النقدي لمقدم الدخول. ويظهر هذا المقابل في العلاقة بينهما على صورتين؛ الأولى ثمن البرامج وأدوات التوصيل التي قام مقدم خدمة الدخول بتوفيرها له؛ ويتم تحديد هذا الثمن في ضوء كمية ونوعية الأجهزة والبرامج التي يحتاج إليها البنك. أما الصورة الثانية فهي الخاصة بمقابل خدمة الدخول، والتي يلتزم البنك بأدائها في صورة اشتراك غالبا ما يكون شهريا، ويراعى في تحديد هذا المقابل سرعة الإنترنت التي سيوفرها مقدم خدمة الدخول للبنك، وكذلك المدة التي سيتاح فيها للبنك الدخول على

---

(١) د. **أسامة أبو الحسن مجاهد**، خصوصية التعاقد عبر الانترنت، دار النهضة العربية، ٢٠٠٣، ص ٥٧.

شبكة الإنترنت خلال اليوم[1].

ب) يلتزم البنك الإلكتروني بالاستعمال الشخصي لخدمة الدخول؛ بمعنى أن خدمة الدخول بما تقتضيه من استعمال خط الاتصال، وكلمة المرور يجب أن تكون مقصورة على البنك فقط، فلا يقوم مثلا بإخراج خطوط إضافية متفرعة عن الخط الأساسي المقدم له من مقدم الخدمة، ولا يقوم بإعطاء كلمة المرور لشخص من الغير، كل ذلك ما لم يتم الاتفاق على غير ذلك[2]. ويعد هذا من أهم الالتزامات التي سيحرص عليها مقدم خدمة الدخول؛ حيث إن له حدًا معينًا من الخطوط يقوم بتوزيعه على المشتركين لديه بحسب السرعة المخصصة له، بحيث إذا ما تجاوز الحد المسموح له فإن ذلك يؤثر بالسلب على السرعة التي يستفيد منها باقي المشتركين، لذلك فهو يحرص على إبرام

---

(١) انظر عقد الاشتراك في خدمة الدخول على شبكة الانترنت لشركة بركوم، متاح على العنوان التالي:

http://arabic.procom.dz/abonnement.htm

(٢) فقد ورد النص في **عقد الاشتراك في خدمة الدخول على شبكة الانترنت لشركة بركوم** سالف الذكر، في البند الثالث من شروط الاشتراك:

- ان الخدمات الممنوحة للمشترك خدمات شخصية أو مهنية، لذا يمنع منعا باتا إعطاء أو تحويل عقده إلى أي شخص آخر أو مؤسسة أخرى بدون إذن خطي من المانح. ولا يجوز بأي حال تقاسم الحساب الشخصي مع أشخاص آخرين أو مؤسسات أخرى.
- سوف يتحمل المشترك كافة المسؤوليات والأخطار التي يمكن أن تنجم عن إفشاء كلمة المرور إلى الخدمات سواء ما تعلق منها بالبريد الإلكتروني أو المعلومات والمعطيات التي تعتبر سرية بالنسبة إليه. انظر العنوان التالي:

http://arabic.procom.dz/abonnement.htm

* **نص أيضا عقد خدمة الانترنت لشركة سوداتل**، في المادة الثانية، فقرة (٢) على (لا يجوز للمشترك إجراء أي تغيير أو أي إضافة في خط الخدمة أو التنازل عنه أو التصرف فيه أو نقله من موقعه الذي تم تركيبه فيه بواسطة سوداتل إلا بموافقة مسبقة مكتوبة وبعد سداد الرسوم المقررة.

البنك بالاستعمال الشخصي لخدمة الدخول.

ج) يلتزم البنك الإلكتروني باستعمال خدمة الدخول لشبكة الإنترنت وفقا للضوابط التي يحددها له مقدم الخدمة، سواء تعلقت هذه الضوابط بطريقة استعمال الخدمة؛ كما لو حظر مقدم الخدمة على البنك الدخول إلى المواقع غير المشروعة أو تحميل برامج أو ملفات محظورة عبر خط الاتصال. أيضا قد تتعلق الضوابط بنطاق أستعمال الخدمة؛ كما لو فرض مقدم الخدمة على البنك عدم استعمال الخدمة بشكل مكثف على نحو قد يؤثر على استفادة المشتركين الآخرين لدى مقدم خدمة الدخول[1].

- مسؤولية الأطراف المتعاقدة:

بالنظر إلى حداثة عقد الدخول على شبكة الانترنت في معاملات البنوك، وبعد التعرض لأهم صور الالتزامات في علاقة الاطراف المتعاقدة، تبدو أهمية التعرف على احكام مسؤولية هذه الاطراف، وذلك على النحو التالي:

(١) فقد ورد النص في **عقد الاشتراك في خدمة الدخول على شبكة الانترنت لشركة بركوم** سالف الذكر، في البند الرابع، والخامس من شروط الاشتراك:

" من أجل تحقيق سيولة وسهولة في الخدمات ومن أجل الصالح العام للمشتركين فإن كل مشترك مطالب بما يلي:

- الاتصال بالخدمة عن طريق مودم واحد.
- عدم الاستعمال المكثف للخدمات من ناحية المدة والسماح للمشتركين الآخرين بالدخول وذلك بعدم ترك الاتصال أكثر من عشرين دقيقة بعد الانتهاء.
- أن المشترك مطالب باحترام القواعد التي تنظم انترنيت بشكل عام لذا يمنع إرسال كافة الرسائل غير المسموح بها والتي تتضمن استفزازات ومضايقات للآخرين من مجتمع الانترنت".

أولا: مسؤولية مقدم خدمة الدخول في مواجهة البنك الإلكتروني:

٦٣- يسأل مقدم خدمة الدخول في مواجهة البنك الإلكتروني في الأحوال التالية:

- يسأل مقدم خدمة الدخول بموجب قواعد المسؤولية العقدية عن تعويض كافة الأضرار التي تلحق البنك الإلكتروني، والناتجة عن إخلاله بأحد الالتزامات التي تضمنها العقد المبرم بينهم. وتحدد قواعد المسؤولية العقدية لمقدم الخدمة بالنظر إلى طبيعة كل التزام يتضمنه العقد[١]. فالالتزام بتزويد البنك بالأجهزة والبرامج اللازمة لتوصيل البنك بشبكة الإنترنت هو التزام بتحقيق نتيجة، ومن ثم يكفى البنك الإلكتروني هنا أن يثبت عدم تحقق النتيجة المرجوة، دون الحاجة لإثبات خطأ مقدم الخدمة حتى تقوم مسؤولية الأخير، ولا يستطيع مقدم الخدمة في هذه الحالة أن يدفع مسؤوليته إلا بإثبات السبب الأجنبي. أما في حالة الالتزام بتقديم النصائح والإرشادات اللازمة لتشغيل الأجهزة، فهو التزام يغلب عليه أنه التزام ببذل عناية، ومن ثم يجب على البنك الإلكتروني في هذه الحالة أن يثبت خطأ مقدم الخدمة حتى تقوم مسؤوليته العقدية، ويقاس خطؤه في هذه الحالة في ضوء طبيعة الخدمة التي يقدمها للبنك، والمخاطر المحيطة بتقديم الخدمات المصرفية على شبكة الإنترنت، وذلك على النحو الذي يلزم مقدم الخدمة ببذل المزيد من العناية والحرص أثناء تبليغ الإرشادات والتعليمات الخاصة بخدمة الدخول للبنك.

---

(١) ويمكن أن يحدد ما إذا كان تحديد ما إذا كان الالتزام بتحقيق نتيجة أو ببذل عناية من خلال النظر إلى ما اتجهت إليه إرادة المتعاقدين في ذلك في ضوء النتيجة المرجوة من هذا الالتزام. كما أن الصفة المؤكدة أو الاحتمالية للنتيجة تلعب دورا في تحديد طبيعة الالتزام، فإذا كانت النتيجة مؤكدة بحسب المجرى العادي للأمور كنا بصدد التزام بتحقيق نتيجة. أما إذا كانت النتيجة ليست مؤكدة في ظل أي مستوى من العناية، كنا بصدد التزام ببذل عناية. انظر د. **محمد حسين منصور**،مرجع سابق، ص ٨٧.

والسؤال هل يمكن أن تنعقد المسؤولية العقدية لمقدم خدمة الدخول في مواجهة البنك الإلكتروني عن إخلاله بالالتزام بالسلامة؟

سبق أن ذكرنا أن الالتزام بالسلامة هو عبارة عن التزام يفرض على المدين بتنفيذ التزامات العقد دون أن يصيب الدائن بضرر، وأن هذا الالتزام مرتبط بشرطين، الأول/ أن ينطوي العقد على خطر يهدد أحد الطرفين، والثاني/ أن يكون المدين بالالتزام محترفا. وبإعمال هذه الشروط على مقدم خدمة الدخول نجده يسأل عن الإخلال بالسلامة في مواجهة البنك الإلكتروني عند تنفيذ عقد الدخول على شبكة الإنترنت. فمقدم خدمة الدخول محترف في مجال عمله، ويفترض أنه يحتاج إلى مؤهلات حتى يرخص له بممارسة هذا العمل. يضاف إلى هذا أن تنفيذ التزاماته في مواجهة البنك ينطوي على مخاطر، والتي تنجم عن اعتماده على الأدوات الإلكترونية في تنفيذ التزاماته، الأمر الذي يلوح باحتمالية وجود خطر على البنك من تنفيذ العقد.

- يسأل مقدم خدمة الدخول أيضا في مواجهة البنك الإلكتروني في حالة ارتكابه أي خطأ- خارج نطاق الالتزامات العقدية- سبب ضررا للبنك الإلكتروني، وذلك بموجب قواعد المسؤولية التقصيرية. ويجب على البنك الإلكتروني في هذه الحالة أن يثبت هذا الخطأ.

- يسأل مقدم خدمة الدخول عن أي ضرر يلحق بالبنك الإلكتروني من جراء عمل الأجهزة الإلكترونية، التي توجد تحت حراسته، والتي يستعين بها في تقديم خدمات الدخول على شبكة الإنترنت لعملائه، وذلك إعمالا لنص المادة ١٧٨ من القانون المدني المصري والتي تنص على "كل من تولى حراسة أشياء تتطلب حراستها عناية خاصة أو حراسة آلات ميكانيكية يكون مسئولا

عما تحدثه هذه الأشياء من ضرر، ما لم يثبت أن وقوع الضرر كان بسبب أجنبي لا يد له فيه". وكما سبق أن ذكرنا فإن الكمبيوتر والبرامج الملحقة به تعد من الأشياء التي تحتاج إلى عناية خاصة في ضوء طبيعة عملها والظروف المحيطة بها، وبناء عليه إذا أصيب البنك بضرر ناجم عن الأجهزة أو خطوط الاتصال الخاصة بمقدم خدمة الدخول؛ كانقطاع الاتصال بشبكة الإنترنت أثناء ذروة التعامل مع العملاء بسبب عطل أصاب أحد أجهزة مقدم الخدمة (كالجهاز المركزي المتحكم في خطوط ISDN)، فإن مسؤولية مقدم الخدمة بوصفه حارسا تنعقد، دون أن يكلف البنك بإثبات خطأ مقدم الخدمة، حيث أنه مفترض في هذه الحالة، فقط يجب على البنك أن يثبت أن ما لحقه من ضرر كان نتيجة تدخل الأشياء التي في حراسة مقدم خدمة الدخول حتى تنعقد مسؤوليته، ولا يكفى الأخير إثبات عدم صدور خطأ من جانبه، بل يلزم لدفع المسؤولية في هذه الحالة أن يثبت السبب الأجنبي.

- أيضا يسأل مقدم خدمة الدخول عن أي خطأ قام به سبب ضررا لغير المتعاقدين معه، كعملاء البنك الإلكتروني الذين أصيبوا بضرر من جراء حدوث خطأ في اتصال البنك الإلكتروني بشبكة الإنترنت. ويجب على العميل الذي أصيب بضرر من جراء هذا أن يثبت خطأ مقدم الخدمة حتى تقوم مسؤوليته، وذلك طبقا لقواعد المسؤولية التقصيرية.

ثانيا- مسؤولية البنك الإلكتروني في مواجهة مقدم خدمة الدخول:

٦٤- تنعقد المسؤولية العقدية للبنك الإلكتروني عن أي ضرر يصيب مقدم الخدمة نتيجة إخلال البنك بأي التزام نص عليه عقد الدخول المبرم بينهما. فعدم

قيام البنك بأداء أحد الالتزامات المالية الواقعة على عاتقه (كثمن الأجهزة والبرامج، أو الاشتراك الشهري مقابل الخدمة)، أو عدم مراعاته للضوابط التي قررها له مقدم الخدمة في استعماله لخدمة الدخول، يترتب عليه مسؤوليته عن تعويض هذه الأضرار. وخطأ البنك الإلكتروني بالنظر لطبيعة هذه الالتزامات (التزامات بتحقيق نتيجة) خطأ مفترض، حيث يكفى مقدم الخدمة أن يثبت عدم تحقق النتيجة حتى تقوم مسؤولية البنك. ولا يستطيع الأخير دفع هذه المسؤولية إلا بإثبات السبب الأجنبي.

ويسأل البنك الإلكتروني أيضا عن أي خطأ خارج نطاق الالتزامات العقدية سبب ضررا لمقدم الخدمة، وذلك طبقا لقواعد المسؤولية التقصيرية. ويجب على مقدم الخدمة أن يثبت خطأ البنك الإلكتروني حتى يرجع عليه بالتعويض.

ويسأل البنك الإلكتروني كذلك عن أي خطأ يقع من قبل العاملين لديه، تسبب في إلحاق الضرر بمقدم خدمة الدخول، وذلك طبقا لأحكام مسؤولية المتبوع عن أعمال تابعيه(١). فإذا وقع خطأ من قبل أحد العاملين لدى البنك، أثناء قيامه بمهام وظيفته أو بسببها، وكانت بينه وبين البنك علاقة تبعية (عقد العمل)، وتسبب هذا الخطأ في إلحاق الضرر بمقدم خدمة الدخول فأن البنك يسأل عن تعويض هذه الأضرار(١٧٤ مدني). وفي هذه الحالة يملك مقدم خدمة الدخول الرجوع على العامل مباشرة، أو الرجوع عليه وعلى البنك متضامنين. وفي كافة الأحوال يجوز للبنك الإلكتروني الرجوع على هذا العامل بما أداه من تعويض(٢).

والسؤال: هل يمكن لعملاء البنك الإلكتروني الرجوع على البنك بوصفه

---

(1) **Michael D. Scott**; Op. Cit, p. 452.

(٢) د. **أحمد شوقي عبد الرحمن**، مرجع سابق، ص ٣٢٧.

متبوعا في حالة حدوث خطأ من مقدم خدمة الدخول؟

في الواقع لا يملك عملاء البنك الإلكتروني الرجوع على البنك بهذا الوصف، فكما سبق أن ذكرنا التكييف الذي يغلب على هذه العلاقة هو أنها عقد مقاولة، يلتزم فيها مقدم الخدمة بالقيام بعمل نظير أجر.

هذا وقد أكدت الدائرة الاتحادية بمحكمة الاستئناف الأمريكية (United States Court of Appeals for the Federal Circuit) هذا المعنى، حيث ذهبت إلى أنتفاء مسؤولية البنك عن أعمال مقدم خدمة الدخول، لعدم امتلاك الأول القدرة على إصدار الأوامر والتوجيهات الفنية للثاني، ولا يؤثر في ذلك قيام البنك بتزويد مقدم الخدمة ببعض البيانات اللازمة لمباشرة عمله، حيث إن ذلك لا يعني تبعية مقدم خدمة الدخول له على النحو الذي يجعل البنك مسئولا عن أخطائه بوصفه متبوعا[1].

ويترتب على ذلك أن عميل البنك الإلكتروني لا يملك في حالة أن أصابه ضرر من جراء خطأ صدر من مقدم خدمة الدخول إلا الرجوع عليه بموجب قواعد المسؤولية التقصيرية.

---

(1) **United States Court of Appeals for the Federal Circuit,** BMC resources, inc. v. paymentech, L.P 2006-1503, p 14

المطلب الثاني

عقد تصميم موقع إلكتروني للبنك على شبكة الإنترنت

٦٥- يعد عقد تصميم موقع إلكتروني للبنك على شبكة الإنترنت من أهم عقود الخدمات الإلكترونية اللازمة لإنشاء البنك الإلكترونى[١]. وتتجلى هذه الأهمية في أن الموقع الإلكتروني للبنك على شبكة الإنترنت هو بمثابة النافذة التي يطل من خلالها على عملائه؛ حيث يعرض من خلاله عليهم خدماته المصرفية المختلفة مصحوبة بنماذج للتعاقد على هذه الخدمات، كما يستقبل البنك عن طريق هذا الموقع طلبات العملاء المختلفة.

لذلك تبدو أهمية التعرض لتعريف هذا العقد، ومراحل انشاؤه، وطبيعته القانونية، وأهم الالتزامات التي يرتبها ومسؤلية الاطراف المتعاقدة، وذلك على النحو التالي:

٦٦- تعريف عقد تصميم موقع البنك على الإنترنت:

ويعرف عقد تصميم الموقع الإلكتروني للبنك بأنه عبارة عن عقد من عقود الخدمات الإلكترونية، يلتزم مقدم الخدمة فيه بإنشاء موقع للبنك من خلال جهاز الكمبيوتر المملوك له والمتصل بشبكة الإنترنت بحيث يتمكن البنك من التعامل عبر هذا الموقع من خلال هذا الجهاز[٢].

---

(1) **E-Banking,** Federal Financial Institutions Examination Council; Op. Cit., p 3.

(٢) **د. محمد حسين منصور**، المرجع السابق، ص٢٩.

ويعرف الموقع الإلكتروني(Web site) بأنه عبارة عن تجميع لـصفحات الويب (Web pages) الخاصة بموضوع معين أو الخاصة بمنظمة معينة[١].

ويعرف أيضا بأنــه عبــارة عــن واجهــة المــستخدم للتعامــل(user interface)عبر الإنترنت، والذي يكون متاحا من الناحية التشغيلية، وبما يتضمنه من محتويات في صورة صفحات، تعمل تحت عنوان إلكتروني معين[٢].

وبناء عليه فأن الموقع الإلكتروني للبنك هو عبارة عن مجموعة صــفحات إلكترونية (web)، متصلة فيما بينها، حيث تعمل هذه الــصفحات علــى شــبكة الإنترنت، وتدار من خلال الشبكة الداخلية للبنك الإلكتروني.

٦٧- مراحل إنشاء موقع البنك على شبكة الإنترنت:

ويتم إنشاء موقع البنك الإلكتروني على شبكة الإنترنت من خلال صياغة أو تصميم صفحات الموقع. ويتم ذلك من خلال قيام مصمم الموقع بوضع تــصور معين يتلاءم مع الطبيعة المصرفية للموقع، وما يمكن أن يقدمه من خدمات[٣] ثم القيام بتنفيذ هذا التصور. وغالبا ما يستعين المصمم بأحد اللغات المستخدمة فــي صياغة المواقع، والتي من أشهرها لغة HTML[٤]. كما يتم فــي كثيــرٍ مــن

(1) **Michael chissick, Alistair Kelman**, ; Op. Cit., p. xliii.

(2) **Cooley Godeard llp**, Sample website development and hosting agreement, available at: http://eric_goldman.tripod.com/articles/hostingagmt.htm

(3) **S.K Leong, T.Srikanthan, G.S.Hura**; Op, Cit., p. 1537.

(٤) وهي لغة عالمية تعرف باســم (لغــة ترميــز الــنص المرجعــي **(Hyper Text Markup Language**، وهي تستخدم في تصميم صفحات الويــب علــى شــبكة الانترنت، حيث تستطيع برامج التصفح على شبكة الانترنت قراءتها. وتكون في شكل

الأحيان وصل موقع البنك الإلكتروني بصفحات من مواقع أخرى علـــى شـــبكة الإنترنت[1].

٦٨- الطبيعة القانونية لعقد تصميم موقع البنك على شبكة الإنترنت:

يبدو للوهلة الأولى ومن خلال النظر في طبيعة الأداءات المتبادلة من قبـــل طرفي التعاقد، أننا بصدد عقد مقاولة، حيث يلتزم أحد أطرافـــه، وهـــو مـــصمم الموقع بالقيام بعمل معين يتعلق بأداء خدمة معلوماتية بصورة مستقلة عـــن رب العمل، وفي المقابل يلتزم الطرف الآخر وهو البنك الإلكتروني بـــدفع المقابـــل المالي لذلك[2].

ويترتب بموجب هذا العقد عدة التزامات تقع على عاتق طرفيه وذلك علـــى النحو التالي:

نصوص موضوعة بين رموز أو علامات خاصة وهذه الرموز هي التي توجه أي من برامج التصفح على شبكة الانترنت لعرض الوثائق التـــي تتـــألف منهـــا الـــصفحات المرجعية على الشبكة، والعلامات أو الرموز هي مجموعة من التعليمات التي تحـــدد المكونات أو العناصر المختلفة لأي صفحة مرجعية على شبكة الانترنت. انظر **بهـــاء شاهين**، العولمة والتجارة الإلكترونية، الفاروق الحديثة للطباعـــة والنـــشر، الطبعـــة الأولى ١٤٢١ هـــ - ٢٠٠٠ م، ص ١١٧. انظر مزيدًا من التفصيل علـــى كـــل مـــن **العناوين التالية:**

- http://en.wikipedia.org/wiki/HTML ;
- http://www.arabcin.net/modules.php?name=News&file=article&sid=971

(١) كوضع خط اتصال (Link) بالبنك الإلكتروني على المواقع التجاريـــة علـــى شـــبكة الانترنت التي تقدم منتجات أو خدمات معينة على الشبكة، حيث إن وضع هذه الوصلة يسهل على العملاء بعد الحصول على ما يريدونه من منتجات من خلال هذه المواقـــع من تسوية مدفوعاتهم عن طريق الاتصال بالبنك الإلكتروني من خلال هذا الخط.

(٢) د. **محمد حسين منصور**، مرجع سابق، ص٢٩.

أولا- التزامات مصمم الموقع الالكتروني للبنك:

٦٩- يلتزم مصمم الموقع الإلكتروني في مواجهة البنك بعدة التزامات على النحو التالي:

١)- يتقدم التزامات مصمم الموقع الإلكتروني للبنك على شبكة الإنترنت بإنجاز الموقع على النحو الذي يتفق مع طبيعة نشاط البنك على شبكة الإنترنت. ويتفرع عن هذا الالتزام عدة التزامات أخرى وهي:

أ- تقديم كافة الأدوات المعلوماتية اللازمة لعمل الموقع على شبكة الإنترنت. ومن أهم هذه الأدوات شريط للمهام Toolbar، وهو يساعد على التنقل بين صفحات (maneuvering between pages) الموقع المختلفة. ومحرك للبحث (search engines) وهو يساعد على البحث داخل موقع البنك، وبرنامج لتشغيل مستعرض صفحات الويب (Web Browser) وهو عادة ما يكون برنامج (Java applets)(١). ويقترن بهذا الالتزام التزام المصمم بتقديم كافة المعلومات التي يرى حاجة البنك الإلكتروني إليها لإدارة وتشغيل الموقع على شبكة الإنترنت.

ب- يلتزم مصمم الموقع بأنجازه بمواصفات فنية وجمالية ذات أصالة خاصة تتفق وطبيعة عمل البنك من ناحية، وتلائم ما يحتاج إليه العملاء من بساطة وسهولة في التعامل من ناحية أخرى(٢). كل ذلك مع احتفاظ المصمم بكامل

---

(١) انظر نموذجًا لعقد تصميم موقع إلكتروني :

Cooley Godeard llp, Sample website development and hosting agreement, op.cit.

(2) **John Skip Benamati-Mark A. Serva**, Trust and distrust in online

حقوقه على كل عمل مشمول بالحماية القانونية وفقا لقوانين حماية الملكية الفكرية[1]، فكل ما يقوم مصمم الموقع بتصميمه على الموقع من صور أو أشكال أو علامات أو إطارات مما يتضمن على نوع من الابتكار والجدة يحتفظ عليه بكل حقوقه وفقا لما ينظمه قانون حماية الملكية الفكرية في ذلك.

ج - يجب على مصمم الموقع أن يراعى الميعاد المتفق عليه لتسليم الموقع صالح للعمل[2]. ويجب على البنك أن يحرص على تضمين العقد ميعادا معينا لتسليم الموقع جاهزا للعمل، على أن يلتزم مصمم الموقع بدفع غرامة تأخيرية عن المدة التي يتأخر فيها عن تسليم الموقع في الميعاد المتفق عليه.

٢)- يلتزم مصمم الموقع بإجراء أية تعديلات أو إضافات سواء في نظام عمل الموقع ووظائفه، أو في شكله وتصميمه، وذلك بحسب ما يطلب منه البنك. فقد يحتاج البنك بعد الانتهاء من إنشاء الموقع بعض التغييرات في نوعية الخدمات المصرفية المقدمة، أو يحتاج البنك بعد فترة لتبني شكل جديد للموقع، كأسلوب لجذب العملاء، حيث يجب على المصمم أن يستجيب

---

banking: Their role in developing countries, Information technology for development, Vol. 13 (2) 161–175, 2007, p. 165.

(١) **د. محمد حسين منصور**، مرجع سابق، ص٢٩. انظر أيضا نموذجًا لعقد تصميم موقع إلكتروني:

SteelCity Web Services, Web Site Design Agreement, available at: http://www. steelCitywebservices.com/downloads/webagreement.pdf

(2) **Website Design Agreement,** In House Media, available at: http://www.ihm.co.uk/ terms/Design-Terms.pdf.

لذلك[١].

٣)-الالتزام بالقيام بكافة الإجراءات الإدارية اللازمة لتسجيل العنوان الإلكتروني (Domain Name) للبنك، حيث غالبا ما تتضمن عقود إنشاء المواقع الإلكترونية التزاما من قبل مصمم الموقع بالقيام بكافة الإجراءات اللازمة لتسجيل العنوان الإلكتروني الذي سيعمل تحته الموقع الذي سيقوم بأنشائه[٢].

ولا يخفى على أحد الأهمية الفنية والاقتصادية للعنوان الإلكتروني في عمل البنك على شبكة الإنترنت، فهو الوسيلة التي يمكن من خلالها الوصول إلى البنك الإلكتروني، وذلك لمن يريد التعامل معه. كما أنه يلعب دورا كبيرا في تمييز موقع البنك الإلكتروني عن غيره من المواقع الأخرى العاملة على شبكة الإنترنت. وهذه الأهمية تقتضي تسجيل هذا العنوان[٣]. ويتم تسجيل الموقع الإلكتروني من خلال القيام بتقديم طلب يفيد ذلك إلى إحدى الجهات القائمة على تسجيل عناوين المواقع الإلكترونية، وذلك عن طريق ملء استمارة التسجيل Application Form، والتي تكون متاحة على المواقع الإلكترونية الخاصة بهذه الجهات، هذا بالإضافة لدفع الرسوم المقررة من

---

(1) Ibid.

(2) **SteelCity Web Services,** Web Site Design Agreement, available at: http://www. steelCitywebservices.com/downloads/webagreement.pdf

(٣) ويخضع تسجيل العناوين الإلكترونية على شبكة الانترنت لمبدأ الأسبقية في التسجيل، وهو يعنى أن الأحقية في العنوان تكون لمن كان له السبق في تسجيله لدى الجهات المختصة بذلك، وهذا المبدأ يعد بمثابة الشرط الوحيد لتسجيل الموقع. حيث يكاد ينحصر دور الجهة التي تتلقى طلبات التسجيل في مجرد التأكد من عدم سبق تسجيل العنوان المراد تسجيله لشخص آخر.أ نظر في تفصيل ذلك د. **شريف محمد غنام**، حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الإلكتروني، دار النهضة العربية، (بدون تاريخ نشر)، ص١٦.

قبل هذه الجهات لذلك. وتقوم هذه الجهات بوضع القواعد التي تحكم وتنظم عملية تسجيل العنوان الإلكترونى[1].

ويثور بخصوص هذا الالتزام تساؤل يتعلق بالطبيعة القانونية لحق البنك على العنوان الإلكترونى؟ بمعنى أخر هل يتمتع البنك بحق ملكية على هذا العنوان أم هو مرخص له فقط في إستخدامه؟

لا يوجد في النظام القانوني المصري نص قانوني أو حكم قضائي يعطى حلا لهذا التساؤل. لكن من خلال مطالعة موقف النظم القانونية الأخرى تبين أن هذا التساؤل قد تسبب في أنقسام احكام المحاكم إلى اتجاهين، وذلك على النحو التالى:

الاتجاه الأول:

---

(١) ومن أولى الشركات التي عملت في مجال تسجيل العناوين الإلكترونية شركة أمريكية تسمى شركة IANA (Internet Assigned Number Authority)، وقد كانت تحتكر ممارسة هذا النشاط حتى عام ١٩٩٨، حيث حلت محلها شركة (Internet Corporation for Assigned Names)ICANN. وقد قامت هذه الشركة بصياغة القواعد والإجراءات التي تحكم تسجيل العناوين الإلكترونية. وقد قامت هذه الشركة فيما بعد بتفويض بعض الشركات المنتشرة في مناطق متفرقة من العالم بمباشرة اختصاصاتها في تسجيل العناوين الإلكترونية. ففي أوربا الشركة المسؤلة عن هذا النشاط هي شركة RIPENCC ('Resaux IP Europeans Network Coordination Center)، وفي الولايات المتحدة الأمريكية شركة InterNIC (Internet National Information Center)، وفي آسيا شركة (ASIA Pacific Network Information Center)APNIC. **د. شريف محمد غنام**، حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الإلكتروني، المرجع السابق، ص ٢٦؛ انظر أيضا:

Website Design Process, Vivid internet production, available at: http://www. biztree.com/Templates/Website-Design-Agreement.html; **Chris Reed**;Op, Cit, p 44

وقد أخذ بهذا الاتجاه القضاء الأمريكى(١)، والذى ذهب إلى أن البنك يتمتع بحق ملكية على العنوان الإلكتروني، وذلك على النحو الذي يمكن البنك من التصرف في هذا العنوان للغير أو التنازل عنه.

الاتجاه الثاني:

وقد تبنى القضاء الإنجليزى(٢) هذا الاتجاه، حيث ذهب للقول بأن البنك لا يتمتع بحق ملكية على العنوان الإلكتروني، وأن الأمر يتوقف عند حد استخدام العنوان الإلكتروني من قبل الجهة المسؤلة عن تسجيل هذه العناوين بموجب العقد الذي يحكم علاقة البنك بجهة التسجيل. وقد برر هذا القضاء هذا الاتجاه بقياس العنوان الإلكتروني للبنك على رقم التليفون أو عنوان الشارع، في أنها مجرد وسائل للتعريف بالشخص الذي رخص له باستعمالها، ولكن هذا لا يعنى أن له عليها حق ملكية.

ونحن من جانبنا نؤيد الاتجاه الأول، في أن حق البنك على العنوان الإلكتروني حق ملكية وليس مجرد ترخيص باستخدام العنوان الإلكتروني، وذلك للأسباب التالية:

---

(1) **United states court of appeals for the ninth circuit**, (Kremen *v* Cohen), 337 F.3d 1024; 2003 U.S. App. Lexis 14830; 67, No. 01-15899, July 25, 2003, available at:
http://www.nvls.edu/user_files/1/3/4/30/84/85/114/127/1806.pdf

(2) **The court of appeal**, autumn 2006, (Plant *v* Service Direct), available at:
http://henmansllp.com/domain_names

ولم يظهر لنا في هذا الخصوص سوى نص المادة (٩٧) من قانون البنك المركزي رقم ٨٨ لسنة ٢٠٠٣[(١)]، والتي تنص على أن (تكون جميع حسابات العملاء وودائعهم وأماناتهم وخزائنهم وكذلك المعاملات المتعلقة بها سرية، ولا يجوز الاطلاع عليها أو إعطاء بيانات بطريق مباشر أو غير مباشر إلا بإذن كتابي من صاحب الحساب أو الوديعة أو الأمانة أو الخزينة أو من أحد ورثته أو من أحد الموصى لهم بكل أو بعض هذه الأموال، أو من النائب القانوني أو الوكيل المفوض في ذلك أو بناء على حكم قضائي أو حكم محكمين". "ويسرى الحظر المنصوص عليه في الفقرة السابقة على جميع الأشخاص والجهات بما في ذلك الأشخاص والجهات التي يخولها القانون سلطة الاطلاع أو الحصول على الأوراق أو البيانات المحظور إفشاء سريتها طبقا لأحكام هذا القانون، ويظل هذا الحظر قائما حتى ولو انتهت العلاقة بين العميل والبنك لأي سبب من الأسباب".

وعلى الرغم من أن النص السابق لم يخاطب مقدمي الخدمات الإلكترونية صراحة بالالتزام بالسرية، إلا أنهم معنيون به، حيث إن هذا النص لم يقصر هذا الالتزام على العاملين لدى البنك فقط، ولكن أيضا كافة الأشخاص والجهات[(٢)]

(١) **قانون رقم ٨٨ لسنة ٢٠٠٣ بإصدار قانون البنك المركزي والجهاز المصرفي والنقد**، الجريدة الرسمية، العدد ٢٤ مكرر، ١٥ يونيه ٢٠٠٣ (السنة السادسة والأربعون).

Available at: http://www.cbe.org.eg/public/Law%20No.88%20for%202003.doc

(٢) ومثال على ذلك موظفو البنك المركزي وموظفو وزارة الاقتصاد والتجارة الخارجية، وموظفو الجهاز المركزي للمحاسبات، حيث نص القانون رقم ١٦٣ لسنة ١٩٧٥ بشأن قانون البنوك والائتمان والمعدل بالقانون رقم ٣٧ لسنة ١٩٩٢ في المواد ٢٧، ٢٨، ٢٩ بإلزام البنوك العاملة في مصر بتقديم بيانات شهرية عن مراكزها المالية، وأي بيانات يطلبها البنك المركزي، وكذلك موافاة البنك المذكور بأية إيضاحات، أو بيانات

التي يخولها القانون سلطة الاطلاع أو الحصول على الأوراق أو البيانات المحظور إفشاء سريتها طبقا لأحكام هذا القانون.

وقد أيدت ذلك فتوى الجمعية العمومية لقسم الفتوى بمجلس الدولة المصري والصادرة في ١٤/١/١٩٩٤ حيث ذهبت إلى: "وعلى ما تقدم، فإن القانون قد أباح لبعض الأشخاص، بحكم وظيفتهم أو مهنتهم أو طبيعة عملهم، الاطلاع على سجلات وحسابات العملاء وودائعهم، وعليه يكون لأمثال هؤلاء معرفة بيانات عن حسابات العملاء ومعاملاتهم مع البنوك. لذا فقد مد المشرع نطاق الحظر إليهم ومنعهم من إفشاء هذه الأسرار"(١).

وبناء عليه يلتزم مقدمو الخدمات الإلكترونية بالمحافظة على سرية البيانات التي يطلعون عليها بحكم عملهم لدى البنك الإلكتروني العامل عبر شبكة الإنترنت. لكن هذا لا يمنعنا من توجيه النداء للمشرع المصري لضرورة التدخل لمعالجة هذا الأمر بنص خاص يراعى فيه طبيعة البنك العامل عبر شبكة الإنترنت؛ والذي يتركز نشاطه في حركة وتداول البيانات عبر أجهزة إلكترونية، تحتاج إلى تدخل مقدمي الخدمات الإلكترونية في كثير من الأحيان لتشغيل وصيانة هذه الأجهزة، الأمر الذي يحتاج إلى إحداث نوع من التوازن بين

يطلبها، وللبنك المركزي أن يندب موظفا أو أكثر للاطلاع على دفاتر البنك وسجلاته على أن يتم هذا الاطلاع في مقر البنك، وقد خول ذات القانون موظفي وزارة الاقتصاد والتجارة الخارجية حق الإطلاع أيضا. كما نص القانون رقم ١٤٤ لسنة ١٩٨٨ بشأن الجهاز المركزي للمحاسبات في المادتين ٦، ٣، تخول مراقبة الجهاز المركزي للمحاسبات الإطلاع على حسابات العملاء عند فحص ومراجعة أعمال فروع البنك طبقا لنصوص القانون سالف الذكر.

(١) **انظر د. سعد علي أحمد رمضان**، المسؤولية المدنية الناشئة عن الإخلال بالالتزام بالسرية دراسة مقارنة بالفقه الإسلامي، دار النهضة العربية، ٢٠٠٧، ص ٣٤١.

اعتبارات حماية السرية واعتبارات تدخل مقدمي الخدمات الإلكترونية وما يتيحه هذا التدخل من احتمالية الاطلاع على البيانات.

وإلى أن يتم هذا التدخل من قبل المشرع، يجب على البنك أن يؤكد ويشدد على هذا الالتزام في مواجهة مقدمي الخدمات الإلكترونية بصورة عامة، وذلك من خلال تبني سياسة عامة تسري على علاقاته معهم، تقوم هذه السياسة على معايير ثابتة تتمثل فيما يلي[1]:

- أن يحد البنك قدر المستطاع من الكشف، أو السماح بالدخول على أية معلومات أو بيانات إلا بالقدر الذي تقتضيه الضرورة، بحيث تقدر الضرورة بقدرها.
- أن يحظر البنك على مقدمي الخدمة التعامل مع أشخاص يمارسون أنشطة غير مشروعة.
- أن يحظر البنك على مقدمي الخدمة ممارسة أي نشاط يشكل اعتداء على أي عمل محمى بقوانين الملكية الفكرية، خاصة برامج الكمبيوتر.
- أن يشجع البنك مقدمي الخدمة على الإبلاغ عن أية مخالفة تخص سرية البنك وتعاملاته.

يضاف إلى ذلك ضرورة تبنى البنك الإلكتروني لنظام رقابي محكم على أنشطة مقدمي الخدمات الإلكترونية فيما يتعلق بالاطلاع على البيانات الخاصة

---

(1) **Michael D. Scott;** Op. Cit., p. 452; **David L. Baumer and others**; Op. Cit, p. 402; **Bank of internet USA,** Privacy Policy, January 2006, available at: http://www.bankofinternet.com/privacy-policy.aspx

بالبنك وعملائه (1)، وذلك على النحو الذي يراعى فيه الحفاظ على سرية هذه البيانات من ناحية، ويراعى من ناحية أخرى توفير مساحة من الحرية لمقدمي الخدمات على النحو الذي يمكنهم من ممارسة عملهم.

وعلى صعيد التشريعات الأخرى، فالملاحظ عليها أنها أولت اهتماما كبيرا بالتزام مصمم الموقع بالحفاظ على سرية البيانات التي تصل إلى علمه بحكم عمله.

فقد نظمت العديد من التشريعات في الولايات المتحدة الأمريكية على هذا الالتزام، منها قانون سرية الاتصالات الإلكترونية (Electronic Communications Privacy Act)(2)، وقانون حماية السرية على

---

(1) **Michael D. Scott,** Op. Cit, p. 453.

(2) (2) " a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service".

"(B) "solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing". **Electronic Communications Privacy ACT of 1986**, available at: http://www.cpsr.org/issues/privacy/ecpa86

- وتعرف كلمة السرية في اللغة بأنها ما يكتمه المرء في نفسه. وتعرف في الاصطلاح بأنها حصر المعلومة وعدم حركتها إلا في نطاق عدد محدود من الأشخاص. ويبرز أهمية السرية كالتزام يقع على عاتق معظم المتعاملين في التجارة الإلكترونية عبر شبكة الانترنت، خاصة المعاملات المصرفية ما تتمتع به المعلومات من أهمية اقتصادية كبيرة، وذلك على النحو الذي جعل المعلومة وهي شيء غير مادي (بدون النظر إلى الوسيط المادي المحملة عليه) محلا للحقوق المالية، يمكن حيازتها وتداولها والتعامل فيها، ومن ثم كان الالتزام بالسرية هو بمثابة حصن الأمان

الإنترنت(OPPA)، والتي حرصت جميعها على التشديد من التزام مقدمو الخدمات الإلكترونية بسرية كافة البيانات التي تصل إلى علمه، وذلك من خلال تبنى مجموعة من الإجراءات المناسبة (Reasonable procedures)، والتي تكفل سلامة هذه البيانات وعدم الاطلاع عليها من قبل غير المخولين بذلك(١).

أيضا جاء في التوجيهات الأوربية الخاصة بسرية الاتصالات الإلكترونية ما يلزم مقدمي الخدمات الإلكترونية باتخاذ الإجراءات اللازمة لحماية أمن المعاملات وسريتها(٢).

وقد ذهب جانب من الفقه، في سبيل بيان المقصود بالإجراءات المناسبة التي يجب على مقدمي الخدمات الإلكترونية اتخاذها للحفاظ على السرية، بأنها الوسائل الأمنية من التشفير والحوائط النارية والرقابة المستمرة(٣).

ويبدو لنا أن هذا الرأي قد نظر لمفهوم الإجراءات المناسبة من زاوية

بالنسبة لهذه المعلومات. ومن أهم الالتزامات التي يلتزم بها المتعاملون مع هذه المعلومات أيا كانت صفتهم. **د. عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية،الكتاب الثاني- الحماية الجنائية لنظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، ٢٠٠٢، ص ٢٧٨.

(1) **David L. Baumer and others,**; Op. Cit., p. 407; **Everett Durante Cordy,**; Op. Cit, p. 403

(2) EU **directive on privacy and electronic communications**, Official Journal of the European Communities, 2002, article 4. (The provider of a publicly available electronic communications service [an online service provider] must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security)

(3) **David L. Baumer and others,**; Op. Cit., p. 407.

واحدة، وهى الأدوات الفنية اللازمة للحفاظ على السرية، لكنه أغفل زاوية أخرى لا تقل أهمية وهي التنظيم القانوني. فالإجراءات المناسبة التي يجب أن يتخذها مقدم الخدمة يجب أن تشتمل على أمرين: الوسائل الفنية، والتنظيم القانوني؛ والذي يظهر من خلال التزامات ومسؤوليات مشددة يجب أن يلتزم بها مقدم الخدمة والعاملين لديه والمتعاملين معه بالحفاظ على السرية. فالإجراءات والأدوات الفنية مهما كان ما تتمتع به من قدرة وكفاءة من الناحية الفنية، فإنها لا تكفى بدون تنظيم قانوني قوى ودقيق تعكسه العقود التي يرتبط بها مقدم الخدمة.

هذا وقد راعت التشريعات سالفة الذكر إحداث نوع من التوازن بين المصالح المتعارضة لطرفي العقد (البنك الإلكتروني ومقدم الخدمة)، وذلك عندما وضعت للقاضي بعض المعايير التي يجب أن يراعيها عند تقدير الضرر الموجب للمسؤولية المدنية عن الإخلال بهذا الالتزام وهي(١):

- البحث عما إذا كان الاطلاع على البيانات السرية أمرا متعمدا أم لا.
- طبيعة الموقع الإلكتروني (Web)، وطبيعة الأنشطة التي يقدمها.
- مدى الالتزام بالحدود المعقولة والضرورية للتدخل.
- البحث عما إذا كان هناك غرض مشروع من هذا التدخل من عدمه.

ويبدو لنا التوازن في هذه المعايير، حيث إنها قدرت أهمية السرية كالتزام عالق في عنق مقدمي الخدمات الإلكترونية من ناحية، وراعت في ذات الوقت

---

(1) **Scott F. Uhler, Philippe R. Weiss , Michele M. McGee,** Liability Issues and the internet Part 1: Electronic Mail, available at : http://www.lib.niu.edu/ipo/1996/il96. 266.html

طبيعة عملهم التي قد تدفعهم للاطلاع على بعض البيانات السرية، والتي قد يقف وراءها غرض مشروع، أو يكون التدخل غير متعمد، أو يكون هناك تدخل في حدود معقولة ولأسباب معقولة، ومن ثم تكون هذه المعايير قد أحدثت نوعا من التوازن من ناحية أخرى.

والسؤال الذي يطل برأسه علينا يتعلق بطبيعة المعلومات التي يجب الالتزام بالمحافظة على سريتها؟

وتبدو أهمية هذا التساؤل في رسم إطار واضح لنوعية المعلومات التي يشملها الالتزام بالسرية، والتي يعد إفشاؤها انتهاكا لهذا الالتزام. وقد بينت إحدى الدراسات أن المقصود بالمعلومات السرية في نظام عمل البنك الإلكتروني ما يلي(١):

١)- البيانات التي تقتضي طبيعتها السرية؛ وهي على سبيل المثال البيانات المتعلقة بالمعاملات المصرفية.

٢)- البيانات التي يتم الاتفاق بين الأفراد صراحة على سريتها، والتي من أهمها:

أ- كافة البيانات الموجودة داخل أجهزة البنك.

ب- أية بيانات خاصة بمحتوى عناصر الملكية الفكرية.

---

(1) **Transactional banking services conformed Contract**; Op. Cit., p. 2; **Everett Durante Cordy**, Op. Cit, p. 403; **Bank of Internet USA,** Privacy Policy, January 2006, available at: http://www.bankofinternet.com/privacy-policy.aspx

جـ- أية معلومات مشتقة أو مجمعة من معلومات سرية.

وبناءً عليه يجب على مصمم الموقع أن يلتزم بهذا الإطار، ويجب أن يحرص البنك على أن يبين ويحدد له طبيعة هذه المعلومات بصورة صريحة في العقد المبرم بينهما.

ثانيًا: التزامات البنك الإلكتروني:

٧٠- في المقابل يلتزم البنك الإلكتروني بمجموعة من الالتزامات على النحو التالي:

١)- يلتزم البنك الإلكتروني بأن يزود مصمم الموقع بكل المعلومات والبيانات التي يحتاج إليها لإنشاء الموقع. فمصمم الموقع يحتاج إلى تفصيل بأنواع الخدمات المصرفية التي يقوم البنك بتقديمها للعملاء، مصحوبة بنماذج للعقود المرتبطة بكل خدمة. كذلك يجب على البنك أن يختار تركيبة العنوان الإلكتروني التي يريد أن يعمل الموقع تحتها ويقدمها لمصمم الموقع حتى يقوم بتسجيلها لصالح البنك[1].

٢)- يجب على البنك الإلكتروني أن يتأكد من إنشاء الموقع وفقا للمتفق عليه. ويتحقق ذلك للبنك من خلال قيامه بمعاينة الموقع، واختباره قبل استلامه وإنهاء طرف مصمم الموقع، وذلك للتأكد من مراعاة المصمم لكل ما تم الاتفاق عليه[2]. فإذا ما تبين له وجود مخالفات عليه أن يطلب من المصمم

---

(1) **Website Design Agreement**, In house media, available at: http://www.ihm.co. uk/terms/Design-Terms.pdf

(2) **Ibidum..**

أولا- مسؤولية مصمم الموقع الالكترونى:

في ضوء الالتزامات السابقة تنعقد مسؤولية مصمم الموقع الإلكتروني في مواجهة البنك على النحو التالي:

(أ) المسؤولية الجنائية لمصمم موقع البنك الإلكترونى:

٧١- بداية نود أن نسجل أن نصوص قانون العقوبات المصري تخلو من نص خاص ينظم المسؤولية الجنائية لمصمم الموقع الإلكتروني (وغيره من الوسطاء الفنيين)، على الرغم مما يسببه هذا الأمر من فراغ تشريعي، باتت معه الحاجة ملحة إلى وجود نصوص خاصة لتنظيم هذه المسؤولية. وما من سبيل أمامنا إلا محاولة تطويع النصوص العامة في قانون العقوبات لاستيعاب مسؤولية هؤلاء.

وباعتبار أن مصمم الموقع يمكن أن يطلع بحكم طبيعة عمله على بعض البيانات السرية، سواء تم ذلك أثناء إنشاء موقع البنك على شبكة الإنترنت، أو أثناء إجراء إصلاحات في هذا الموقع، فإنه بلا أدنى شك ملتزم بالحفاظ على سرية هذه البيانات. وهذا الالتزام لا تحميه فقط إرادة المتعاقدين من خلال النص صراحة أو ضمنا على ذلك في العقد المبرم بينهما، ولكن يحميه من قبل ذلك المشرع الجنائي.

فقد نص مشروع التجارة الإلكترونية المصري[1] في البند الأول من الفصل العاشر تحت عنوان سرية البيانات المشفرة على تجريم أي فعل من شأنه أن ينال

---

(١) راجع مشروع قانون التجارة الإلكترونية المصري على الموقع الإلكتروني التالي

http://www.f-law.net/law/showthread.php?t=13243

من سرية أو خصوصية البيانات، وذلك بكشف مفاتيح التشفير، أو إساءة استخدامها بأي صورة من الصور، كما عاقب أيضا كل من يقوم بفض معلومات مشفرة في غير الأحوال المصرح بها قانونا.

ويلاحظ على هذا النص أمران:

الأول: أنه قصر الحماية الجنائية على البيانات المشفرة دون غيرها، على الرغم من أن التشفير أحد الوسائل المتبعة لحماية البيانات، وليس كلها. فهناك الجدار الناري (Fire walls)، ووسائل التحكم في الدخول (Access Controls)، وغيرها من وسائل حماية البيانات[1]، ومن ثم يجب أن يكفل هذا النص حماية البيانات متى كانت سرية، بغض النظر وسيلة الحماية المتبعة[2].

الثاني: أن النص السابق خاص بمشروع قانون لم ير النور بعد، الأمر الذي يدفعنا إلى البحث في القواعد العامة عن علاج لهذه المشكلة العضال.

فقد نص القانون رقم ٢٠٥ لسنة ١٩٩٠ في شأن سرية الحسابات البنكية في المادة الأولى منه على أن "تكون جميع حسابات العملاء وودائعهم وأماناتهم وخزائنهم في البنوك، وكذلك المعاملات المتعلقة بها سرية، ولا يجوز الاطلاع عليها أو إعطاء بيانات عنها بطريق مباشر أو غير مباشر....".

كما نصت المادة الخامسة من ذات القانون على أنه " يحظر على رؤساء وأعضاء مجالس إدارة البنوك ومديريها أو العاملين بها إعطاء أو كشف أية

---

(1) **Thomas C. Glaessner- Tom Kellermann -Valerie McNevin,** Electronic safety and Soundness, world bank working, paper no.26, 2004, p. 66.

(٢) **د. عبد الفتاح بيومي حجازي**، مرجع سابق، ص ٢٨٤.

معلومات أو بيانات عن عملاء البنوك أو حساباتهم أو ودائعهم أو الأمانات أو الخزائن الخاصة بهم أو معاملاتهم في شأنها أو تمكين الغير من الاطلاع عليها في غير الحالات المرخص بها بمقتضى أحكام هذا القانون.

ويسرى هذا الحظر على كل من يطلع بحكم مهنته أو وظيفته أو عمله بطريق مباشر على البيانات والمعلومات المشار إليها".

ويتضح من صياغة هذا النص أنه على الرغم من عدم ذكره الصريح لمصمم الموقع الإلكتروني للبنك ضمن الملتزمين بالسرية، إلا أنه ذكر أن الحظر يشتمل على كل من يطلع بحكم مهنته أو وظيفته أو عمله بطريق مباشر على البيانات والمعلومات المشار إليه. وبناء عليه يلتزم مصمم موقع البنك بالسرية؛ وذلك لما تتيحه له طبيعة عمله من الاطلاع على البيانات الخاصة بالبنك وتعاملاته، سواء أثناء تصميم موقع البنك على شبكة الإنترنت، وما يرتبط بذلك من الاطلاع على بعض المعلومات المتعلقة بالخدمات المصرفية التي يقدمها البنك، وبيانات بالعقود المصرفية التي تحكم تقديم هذه الخدمات، والبيانات اللازمة للدخول على هذه الخدمات والتعامل معها، أو أثناء إجراء إصلاحات لأعطال قد تلحق بهذا الموقع أثناء العمل، حيث قد تهيأ له الفرصة في هذه الأحوال للنفاذ إلى قاعدة البيانات الخاصة بالبنك.

يضاف إلى ذلك نص المادة ٣٠٩ قانون العقوبات المصري، والتي نصت على أن "يعاقب بالحبس مدة لا تزيد على سنة كل من استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص. في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه، ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة، كما

يحكم بمحو التسجيلات المتحصلة عنها أو إعدامها".

و" يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل- ولو في غير علانية- تسجيلا أو مستندا متحصلا عليه بإحدى الطرق المبينة أعلاه، أو كان ذلك بغير رضاء صاحب الشأن. ويعاقب بالحبس مدة خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم التحصل عليها بإحدى الطرق المشار إليها بحمل شخص على القيام بعمل أو الامتناع عنه".

ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها".

ويتضح من صياغة هذا النص أنه جاء بصياغة عامة قادرة على أن تستوعب أي صورة من صور الإخلال التي تقع من قبل منشئ موقع البنك بسرية البيانات التي يطلع عليها بحكم طبيعة عمل، وذلك أيا كان الجهاز الذي استخدمه في تحقيق هذه الأفعال (كل من استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه).

وبناءً عليه يسأل منشئ موقع البنك الإلكتروني جنائيا عن أي إخلال بسرية البيانات الخاصة بالبنك الإلكتروني أو عملائه. فإذا كانت الضرورة تقتضي في بعض الأحيان السماح لمنشئ الموقع بمطالعة بعض البيانات- سواء عن قصد أو بدون قصد- فإن هذه الضرورة تقدر بقدرها، بحيث يلتزم بالمحافظة على هذه البيانات، وإلا قامت مسؤوليته الجنائية.

ويلاحظ أن مثل هذه المسؤولية (المسؤولية عن الإخلال بسرية البيانات)

تضعف فرصة إثارتها في مواجهة مقدم خدمة الدخول على شبكة الإنترنت. ويعود ذلك إلى أن دوره يقتصر على مجرد الأخذ بيد البنك للدخول على شبكة الإنترنت، على نحو لا تتهيأ له الفرصة للاطلاع على أية بيانات. وقد أكد إعلان مؤتمر بون الوزاري الخاص بشبكات المعلومات الدولية (Declaration of the Bonn Ministerial Conference on Global Information (Networks المنعقد في الفترة من ٦-٨ يوليو ١٩٩٧، على أن مقدمي الخدمات الوسيطة أمثال مشغل الموقع ومقدم خدمة الدخول لا يكونون مسئولين عن محتوى الموقع وما يعرض عليه. وعلى ما يبدو موقفهم هذا يبرر بالدور الفني البحت لهؤلاء الوسطاء، والذي يجعلهم بعيدين عن الاطلاع على المعلومات أو البيانات الخاصة بالموقع الأمر الذي يبرر عدم إلزامهم بالسرية[١].

(ب) المسؤولية المدنية لمصمم موقع البنك الإلكتروني:

٧٢- تتشابه المسؤولية المدنية لمصمم موقع البنك الإلكتروني مع المسؤولية المدنية لمقدم خدمة الدخول على شبكة الإنترنت، حيث تنعقد المسؤولية العقدية لمصمم الموقع عن أي إخلال لأي التزام نظمه العقد المبرم بينهما. كما تنعقد المسؤولية التقصيرية لمصمم الموقع عن أي إخلال يقع منه خارج نطاق الالتزامات العقدية، مما يسبب ضررا للبنك الإلكتروني. كما يسأل أيضا عن أي ضرر يلحق بالبنك الإلكتروني من جراء عمل الأجهزة التي قام بتزويد البنك بها حتى ولو لم يصدر عنه خطأ، وذلك وفقا للتفصيل الذي سبق ذكره بخصوص

(1)**Chris Reed**; Op. Cit., p. 122.

المسؤولية المدنية لمقدم خدمة الدخول على شبكة الإنترنت[١].

يضاف إلى ذلك انعقاد المسؤولية العقدية لمصمم الموقع في مواجهة البنك عن الإخلال بالالتزام بالسرية. والتزام مصمم الموقع في هذه الحالة سيكون التزامًا بتحقيق نتيجة، ولا يكفى منه مجرد ببذل عناية في هذا الصدد، ومن ثم تنعقد مسؤوليته في مواجهة البنك لمجرد عدم تحقق النتيجة المرجوة؛ من خلال انتهاك سرية البيانات الخاصة بالبنك.

أيضا تنعقد المسؤولية التقصيرية لمصمم الموقع في مواجهة عملاء البنك عن إهماله في المحافظة على سرية البيانات الخاصة بهم، وذلك وفقا لحكم المادة (١٦٣ مدني مصري). أيضا أكد القانون الأمريكي (Common Law) على هذا المعنى من خلال النص على المسؤولية التقصيرية لمصمم الموقع بسبب سلوكه المهمل (Negligent behavior) وتقصيره في اتخاذ الإجراءات المناسبة (Reasonably prudent measures) بالحفاظ على سرية البيانات[٢].

ثانيا- مسؤولية البنك الإلكتروني تجاه مصمم الموقع:

في ضوء الالتزامات الواقعة على عاتق البنك في مواجهة مصمم الموقع، تنعقد مسؤولية البنك على النحو التالي:

(أ) المسؤولية الجنائية للبنك الإلكتروني:

٧٣- الالتزام الواقع على عاتق مصمم موقع البنك بانجازه بمواصفات فنية وجمالية ذات أصالة قد يجعله يأتي ببعض التصميمات الخاصة لصفحات الموقع

(١) انظر سابقا، ص ١٤٧.

(2) **David L. Baumer and others,**; Op. Cit., p. 409.

أو الرسوم أو الأشكال التي يحتويها هذا الموقع، والتي تتميز بنوع من الجدة والابتكار من قبل مصممها (وغالبا ما سيطلب منه البنك ذلك نظرا لأن استخدام مثل هذه التصميمات أو الأشكال في عرض الخدمات التي يقدمها البنك من شأنه أن يساهم كنوع من الدعاية في جذب العملاء للتعامل مع البنك)، على نحو يخضع هذه التصميمات للحماية بموجب قوانين حماية الملكية الفكرية[1]، الأمر الذي يلزم البنك الإلكتروني والعاملين لديه بمراعاة هذا.

وبناءً عليه، يسأل البنك الإلكتروني، والعاملين لديه، وعملاؤه جنائيا بموجب نص المادة ١٨١ من قانون الملكية الفكرية المصري والتي تنص على أنه "مع عدم الإخلال بأي عقوبة أشد في قانون آخر يعاقب بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن خمسة ألاف جنيه ولا تزيد على عشرة ألاف جنيه، أو بإحدى هاتين العقوبتين، كل من ارتكب أحد الأفعال الآتية:

- بيع أو تسجيل مصنف أو تسجيل صوتي أو برنامج إذاعي محمي طبقا لأحكام هذا القانون أو طرحه للتداول بأي صورة بدون إذن كتابي مسبق من المؤلف أو صاحب الحق المجاور.
- تقليد مصنف أو تسجيل صوتي أو برنامج إذاعي أو بيعه أو طرحه للتداول أو

---

(١) **انظر المادة ١٤٠ من القانون المصري رقم ٨٢ لسنة ٢٠٠٢ بإصدار قانون حماية الملكية الفكرية**، والتي تنص على أن تتمتع بحماية هذا القانون حقوق المؤلفين على مصنفاتهم الأدبية والفنية وبوجه خاص المصنفات الآتية:

٩- مصنفات الرسم بالخطوط أو بالألوان والنحت والطباعة على الحجر وعلى الأقمشة وأية مصنفات مماثلة في مجال الفنون الجميلة.

١٠- المصنفات الفوتوغرافية وما يماثلها.

١٢- الصور التوضيحية والخرائط الجغرافية والرسومات التخطيطية ....

Katyal, Neal Kumar;Op.Cit, p 41; **William Gram**; Op. Cit, p. 24.

للإيجار مع العلم بتقليده.

التقليد في الداخل لمصنف أو تسجيل صوتي أو برنامج إذاعي أو أداء محمى طبقا لأحكام هذا القانون عبر أجهزة الحاسب الآلي أو شبكات الإنترنت أو شبكات المعلومات أو شبكات الاتصالات أو غيرها من الوسائل بدون إذن كتابي مسبق من المؤلف أو صاحب الحق المجاور.

- التصنيع أو التجميع أو الاستيراد بغرض البيع أو التأجير لأي جهاز أو وسيلة أو أداة مصممة أو معدة للتحايل على حماية تقنية يستخدمها المؤلف أو صاحب الحق المجاور كالتشفير أو غيره.
- الاعتداء على أي حق أدبي أو مالي من حقوق المؤلف أو الحقوق المجاورة المنصوص عليها في هذا القانون.

ويضاف إلى العقوبات الأصلية سابقة الذكر بعض العقوبات التكميلية التي نصت عليها ذات المادة (١٨١ سالفة الذكر)، وهي إمكانية قيام المحكمة بمصادرة النسخ محل الجريمة أو المتحصلة منها، وكذلك المعدات والأدوات المستخدمة في ارتكابها، كذلك للمحكمة أن تغلق المنشأة التي تم استغلالها في ارتكاب الجريمة مدة لا تزيد على ستة أشهر.

(ب) المسؤولية المدنية للبنك الإلكتروني:

٧٤- يسأل البنك الإلكتروني مدنيا في مواجهة مصمم الموقع طبقا لما هو مقرر في خصوص مسؤوليته في مواجهة مقدم خدمة الدخول، لذلك نحيل بشأنها لما سبق ذكره بخصوص المسؤولية المدنية لمقدم خدمة الدخول، وذلك منعا للتكرار.

المطلب الثالث

عقد إيواء موقع البنك على شبكة الإنترنت

٧٥- يمثل عقد إيواء الموقع الإلكتروني للبنك على شبكة الإنترنت أهمية كبيرة. وتظهر هذه الأهمية في طبيعة الخدمة التي يحصل عليها البنك من وراء مقدم خدمة الإيواء، والتي تتمثل في إيواء وتسكين موقعه على شبكة الإنترنت، والقدرة على التعامل مع هذا الموقع الذي يحتوى على البرامج والملفات الخاصة به عبر شبكة الإنترنت؛ فالبنك بعد أن ينتهي من تصميم موقعه، تظهر له الحاجة في أن يأوي إلى مكان خاص به في هذا العالم الافتراضي، ومن ثم فهو في حاجة إلى عقد يوفر له هذه الخدمة. لذلك سوف نعرض في هذا المطلب لتعريف هذا العقد، وطبيعته القانونية، وأهم الالتزامات التي يرتبها، والمسؤوليات الناشئة عنها، وذلك على النحو التالي:

أولا: تعريف عقد إيواء موقع البنك على شبكة الإنترنت:

٧٦- تعرض التوجيه الأوربي رقم (٢٠٠٣/٣١) في المادة (١٣) لتعريف خدمة الإيواء، فعرفها بأنها عبارة عن تخزين آلي ووسيط ومؤقت للمعلومات، يتم لتسهيل تقديم عملية إرسال هذه المعلومات بكفاءة(١).

ويعرف عقد تقديم خدمة الإيواء، بأنه أحد عقود الخدمات الإلكترونية التي يلتزم بموجبها متعهد الإيواء بتخصيص جانب من أدواته الفنية (جهاز كمبيوتر

---

(1) **Stephen Rawson ,Denton Wilde Sapte;** Op. Cit., p. 168.

يعمل كخادم[1] (Dedicated server computers) لاستضافة أو تسكين موقع البنك الإلكتروني، وذلك نظير التزام البنك بدفع المقابل المتفق عليه[2].

وعرف بعض الفقه كذلك هذا العقد بأنه ذلك الذي يلتزم بمقتضاه مقدم خدمة الإيواء بأن يضع تحت تصرف البنك الإلكتروني جانبا من إمكانياته الفنية، كي يستعملها الأخير في تحقيق مصالحه وبالطريقة التي تناسبه، وذلك من خلال إتاحة الفرصة للبنك في الدخول على شبكة الإنترنت، وتيسير استخدام موقعه الإلكتروني الذي خزن فيه معلوماته[3]. ويطلق على مقدم خدمة الإيواء أسماء عدة منها "مورد الإيواء"، و"المورد المستضيف"، و"متعهد الإيواء" إلا أن المصطلح الأخير هو أكثر المصطلحات التي تطلق عليه[4].

٧٧- وتتلخص طبيعة عمل متعهد الإيواء في قيامه بتخصيص مساحة لاستضافة وإيواء المواقع الإلكترونية على أجهزة الكمبيوتر الخاصة به[5] التي تعمل

---

(١) وهذا الخادم عبارة عن جهاز كمبيوتر ذي مواصفات خاصة، ونظام تشغيل خاص يعمل على تخزين البرامج والملفات التي تشكل مادة المواقع الإلكترونية ليتمكن المتعاملون مع هذه المواقع من تصفحها عبر الانترنت.انظر هذا التعريف على الموقع التالي:

http://www.libyanspider.com/arabic/hosting/hostingfaq.php

(2) **Website hosting contract and terms of service agreement**, available at: https://secure7.hostek.net/contract.shtml

(٣) د. محمد حسين منصور، مرجع سابق، ص ٢٧

(٤) انظر د. شريف محمد غنام، التنظيم القانوني للإعلانات التجارية عبر شبكة الانترنت، المرجع السابق، ص١٧.

(٥) (ويشبه البعض هذه الخدمة بشخص يملك عقارا ما ويطرحه للإيجار. فبعد أن قام هذا المالك ببناء العقار، يعرضه لأي شخص يرغب في الحصول على مكان بالإيجار ممن لا يستطيعون بناء أو شراء عقار خاص بهم، وذلك مقابل مبلغ معين، ويكون في إمكانهم الإقامة في العقار وتغييره وتأثيثه بما يتناسب مع أذواقهم وحاجاتهم، ويكون

كخوادم (servers)، وتكون متصلة بشبكة الإنترنت،[1] هذه الخوادم لها القدرة على إرسال واستقبال المعلومات عبر شبكة الإنترنت، ومن ثم البنك الإلكتروني سيتعاقد مع متعهد الإيواء على تخصيص مساحة من أجهزته لإيواء موقع البنك على شبكة الإنترنت، والتعامل مع هذا الموقع من خلال هذه الأجهزة.

٧٧- ويجب على البنك الإلكتروني أن يراعى مجموعة من الأمور عند اختياره لمتعهد الإيواء الذي سيقوم بالتعاقد معه، منها[2]:

- أن يقدر حجم موقعه الإلكتروني، ومن ثم السعة التخزينية التي سيحتاج إليها. ويقدر حجم الموقع في ضوء عدد صفحاته (Webs)، وما تشتمل عليه هذه الصفحات من صور وملفات صوت وفيديو.
- تقدير نسبة زوار الموقع المتوقعة، وأوقات الكثافة في التعامل مع الموقع. وذلك حتى يمكن تحديد السرعة المطلوبة لنقل البيانات.
- تحديد عدد صناديق البريد الإلكتروني (E- Mail Box) التي سوف يستعملها لموقعه.

أمر صيانة البيت من مسؤولية المالك. فالأمر نفسه في خدمة استضافة المواقع، حيث تقوم شركات الاستضافة بتأجير مساحة معينة على أجهزة الخادم الخاصة بها لمواقع مختلفة، وكل موقع له شكله وحجمه الخاص، بينما تكون مسؤولية صيانة الخادم هي من مسؤولية شركة الاستضافة. انظر العنوان التالي:

http://www.libyanspider.com/arabic/hosting/hostingfaq.php; **Chris Reed,**; Op. Cit, p. 19.

(1) **Website hosting contract and terms of service agreement**, Op. Cit.

(2) Available at:http://www.libyanspider.com/arabic/hosting/hostingfaq.php; **Chris Reed**; Op. Cit., p. 19.

وترجع أهمية هذه الأمور السابقة إلى أنها تساعد البنك الإلكتروني على اختيار متعهد إيواء يتمتع بقدرات تتناسب مع احتياجاته، وطبيعة تعاملاته على شبكة الإنترنت، الأمر الذي سينعكس على حسن أداء البنك، وتفاعله مع العملاء عبر شبكة الإنترنت.

ثانيا: الطبيعة القانونية لعقد إيواء موقع البنك على شبكة الإنترنت:

٧٨- اختلف الفقهاء في تحديد الطبيعة القانونية لعقد إيواء موقع البنكِ على شبكة الإنترنت، وانقسموا في ذلك إلى عدة اتجاهات.

فقد ذهب أنصار الاتجاه الأول[١] إلى القول بأنه عقد إيجار أشياء. ويعلل هذا الجانب موقفه بأن جوهر الخدمة التي يقوم متعهد الإيواء بتقديمها لمتلقي الخدمة (البنك)، هي إتاحة الانتفاع بأجهزته، نظير التزام الأخير بدفع مبلغ معين.

على الجانب الآخر ذهب البعض[٢] إلى تكييف هذا العقد على أنه عقد مقاولة، واستند في قوله إلى أن الغرض الجوهري من هذا العقد ليس تأجير الآلة أو الجهاز، بل هو العمل أو الخدمة التي يقدمها متعهد الإيواء لمتلقي الخدمة، حيث إنه بدون هذا العمل أو الخدمة ليس ثمة قيمة للجهاز أو للآلة.

وذهب فريق ثالث من الفقه[٣] إلى تبني اتجاه مخالف لما سبق، حيث يرى أن الأفضل بالنسبة لعقد الإيواء أن يكيف على أنه عقد من العقود غير المسماة،

---

(١) **د. محمد حسين منصور**، مرجع سابق، ص٢٨.
(٢) **د. أسامة أحمد** بدر، حماية المستهلك في التعاقد الإلكتروني، دار الجامعة الجديدة للنشر، ٢٠٠٥، هامش ص١٢٤.
(٣) **د. محمد عبد الظاهر حسين**، المسؤولية القانونية في مجال شبكات الانترنت، مرجع سابق، ص ٨٣.

يستمد أحكامه من البنود التي يتفق عليها الأطراف المتعاقدة، ومن أحكام القواعد العامة في القانون. ويضيف أنصار هذا الرأي كذلك أنه لا يمكن قبول وصف عقد الإيواء بأنه عقد إيجار، وذلك لغياب فكرة الالتزام بالضمان التي يلتزم بها المؤجر وفقا لأحكام قانون الإيجار؛ حيث لا يسأل متعهد الإيواء غالبا عن المحتوى غير المشروع للموقع المستضاف، كما لا يسأل عن منع الغير من التعرض باعتبار أنه يتعاقد مع أكثر من مستخدم على موقع واحد.

٧٩- وعلى الرغم من تسليمنا الشديد بوجاهة جميع الآراء السابقة، يبدو الاتجاه الأول الذي يرى أنصاره أن عقد الإيواء هو عقد إيجار قد حالفه الصواب، وذلك للأسباب التالية:

١) أن جوهر ولب التزامات متعهد الإيواء في مواجهة البنك الإلكتروني هو تخصيص مساحة من الأجهزة والمعدات التي يمتلكها لتسكين البنك وإيوائه وانتفاعه بها لمدة معينة[1]، وذلك مقابل أجرة دورية عن مدة الانتفاع، بما يتحقق معه أهم التزامات عقد الإيجار. ولا يخل بذلك قيام متعهد الإيواء بتشغيل ومتابعة عمل الأجهزة التي ينتفع بها البنك، فالمؤجر ملتزم بموجب عقد الإيجار ليس فقط بتسليم العين المؤجرة للمستأجر، ولكن أيضا بتمكينه من الانتفاع بهذه العين بشكل هادئ ومستقر، بما يقتضيه ذلك من تسليمه العين المؤجرة في حالة يمكنه الانتفاع بها، والقيام بإجراء كل ما تحتاج إليه من صيانة على نحو يجعلها صالحة للانتفاع.

٢) لا يمكن القول بغياب فكرة الضمان في عقد إيواء موقع البنك الإلكتروني

---

(1) Chris Reed; Op. Cit, p. 19.

على شبكة الإنترنت، على زعم من القول بعدم مسؤولية متعهد الإيواء عن المحتوى غير المشروع للموقع المستضاف. ففكرة الضمان التي تهيمن على عقد الإيجار تقوم على التزام المؤجر بمنع تعرضه الشخصي، أو تعرض الغير للمستأجر أثناء انتفاعه بالعين، وضمان العيوب الخفية فيها(١)، ولا تتطرق من قريب أو بعيد لمسؤولية المؤجر عن المحتوى غير المشروع للعين المؤجرة .هذا من ناحية، ومن ناحية أخرى لا يمكن أن نطلق القول بعدم مسؤولية متعهد الإيواء عن المحتوى غير المشروع للموقع المستضاف. فالعديد من القوانين تنظم مسؤوليته عن ذلك في حالات، وبشروط معينة(٢). أما بخصوص تعاقد متعهد الإيواء مع أكثر من مستخدم

---

(١) د. **أحمد السعيد الزقرد**، الوجيز في عقد الإيجار، (بدون دار نشر)، ٢٠٠٠-٢٠٠١، ص ١٢٨.

(٢) وهذا ما قرره التوجيه الأوربي رقم (٣١/ ٢٠٠٠)، ومن بعده العديد من القوانين الأوربية، حيث حرصت هذه القوانين على تقليص مسؤولية متعهدي الإيواء عن مشروعية المواد التي تحتويها المواقع التي يستضيفونها. ويتضح ذلك من تعليق إعفائهم من المسؤولية بشروط معينة، وهي:

١ - عدم المعرفة الفعلية بالأنشطة أو المعلومات غير المشروعة، كما أنهم في حالة معرفتهم بوجود مثل هذه المواد المحظورة يسارعون لتعطيل الوصول إليها وإزالتها.

٢- ألا يكون متلقي الخدمة يعمل تحت سلطة ورقابة متعهد الإيواء.

وبمفهوم المخالفة تنعقد مسؤولية متعهد الإيواء عن المحتوى غير المشروع للموقع المستضاف في حالة إذا ما كان على علم ودراية بهذا المحتوى، أو كان صاحب الموقع يقوم بعرض هذه المواد تحت رقابة وإشراف متعهد الإيواء.

- أيضا ذهب القضاء الأمريكي في العديد من أحكامه إلى مسؤولية متعهد الإيواء عن عدم مشروعية المواد التي تعرض على المواقع التي يستضيفها،و ذلك بحكم واجب الرقابة المفروض عليه في هذا الخصوص. انظر في ذلك:

Chris Reed; Op. Cit., p134; **Michael D. Scott**; Op. Cit, p. 451; **Mark Turner and Mary Traynor, Herbert Smith**; Op., Cit, p. 114; **Jonathan A. Friedman- Francis M. Buono,** Limiting tort liability for online third-party content under section 230 of the

على موقع واحد على نحو تنتفي معه فكرة التعرض من قبل الغير، فهذا أمر مردود عليه بأن البنك الإلكتروني، بحكم طبيعة عمله، حريص كل الحرص على أن يخصص له متعهد الإيواء مساحة خاصة به دون أن يشترك معه أي موقع آخر فيها، نظرا لطبيعة العمليات المصرفية، وما تحتاج إليه من سرية وخصوصية.

٣) وعلى ما يبدو أن اللجوء إلى فكرة العقد المسمى هي من قبيل الهروب من إيجاد قالب قانوني مناسب يسع عقد الإيواء. فإيجاد قالب مناسب لعقد ما خاصة إذا كان من الحداثة بمكان أمر من شأنه أن يساعد على سد ثغرات يمكن أن يغفل الأطراف عن معالجتها أثناء إبرام العقد. يضاف إلى ذلك أنه يضع رؤية واضحة أمام القضاء بخصوص ما ينشأ عن هذه العقود من منازعات الأمر الذي يساعد في حل هذه المنازعات.

ولهذا نميل إلى القول بأن هذا العقد عقد إيجار خدمات إلكترونية، ومن ثم ينعكس هذا التكييف القانوني على طبيعة التزامات الأطراف ومسؤولياتهم، وذلك على النحو التالي:

ثالثا- التزامات الأطراف المتعاقدة:

عقد الإيواء عقد تبادلي ينبثق عنه العديد من الالتزامات المتبادلة في العلاقة

Communications Act, Federal communications law journal, Vol. 52, 2005, p 648

انظر تفصيل مسؤولية متعهد الإيواء عن عدم مشروعية الإعلانات التي تعرض على الموقع الذي يستضيفه د. **شريف محمد غنام**، التنظيم القانوني للإعلانات التجارية عبر شبكة الانترنت، مرجع سابق، ص ١٧١.

بين متعهد الايواء والبنك الالكترونى، وذلك على التفصيل التالي:

١)- التزامات متعهد الإيواء في مواجهة البنك الإلكترونى:

٨٠ - يلتزم متعهد الإيواء بمجموعة من الالتزامات في مواجهة البنك الإلكتروني بموجب عقد الإيواء على النحو التالي:

أ- يأتي في مقدمة الالتزامات الواقعة على عاتق متعهد الإيواء في مواجهة البنك الإلكتروني تمكين الأخير من الانتفاع بأجهزته وبرامجه، على نحو يستطيع البنك معه التعامل مع موقعه عبر شبكة الإنترنت. ويتحقق ذلك من خلال قيام متعهد الإيواء بتوفير مساحة للموقع الإلكتروني للبنك على الخادم المملوك له، بالإضافة إلى برنامج لتشغيل خادم الويب (Run web server software)[١]، بحيث يتمكن البنك الإلكتروني من خلال هذا البرنامج من الدخول على مصدر موقع البنك على شبكة الإنترنت[٢]، ومن ثم إمكانية التعامل معه. كما يمكن أن يتبع متعهد الإيواء أسلوبا آخر مع البنك لتمكينه من التعامل مع الموقع وذلك من خلال تزويد البنك بكلمة مرور خاصة للتحكم في الموقع (password controlled FTP)[٣]. ويجب أن يراعى متعهد الإيواء وجود هذه الأجهزة في حالة تكون معها صالحة للاستعمال وفقا للغرض من العقد. ويجب على متعهد الإيواء كذلك

---

(1) **Chris Reed**, Op. Cit., p. 28.

(٢) ويتم ذلك من خلال قيام متعهد الإيواء بتزويد البنك الإلكتروني بما يسمى المفتاح العام للبناء (Public Key Infrastructure) حيث يتمكن البنك من خلال هذا المفتاح من الدخول إلى الموقع الإلكتروني للبنك والتعامل معه. انظر:

Richard H. Paine, Secure mobile architecture (SMA– A way to fix the broken Internet),Information on security technical report, Vol 12, Issue 2, 2007, Pages 85-89.

(3)**Chris Reed**, Op. Cit, p. 28.

تمكين البنك من استعمال هذا الموقع وإدارته بحرية تامة، وذلك بفتح الموقع أو حجبه، أو بإضافة موضوعات أو حذفها على النحو الذي يراه البنك محققا لمصلحته[١].

ويعد هذا الالتزام التزاما بتحقيق نتيجة، فلا تبرأ ذمة متعهد الإيواء في مواجهة البنك إلا بتمكينه من استعمال أجهزته بالفعل من خلال وضعها تحت تصرفه في حالة يستطيع البنك أن يستفيد منها، ولا يكفى مجرد بذل العناية لذلك.

ب- يلتزم أيضا متعهد الإيواء بحكم طبيعة عقد الإيواء (كعقد إيجار خدمات إلكترونية) بأن يضمن للبنك الإلكتروني استمرار الانتفاع بخدماته طوال مدة العقد. وهذا يقتضى قيامه بمتابعة تلقى البنك للخدمة بشكل ميسر، وذلك من خلال مراقبة عمل الأجهزة من الناحية الفنية، وصيانتها بشكل دوري، وعدم استضافة مواقع أكثر مما تستوعب طاقة الخوادم على نحو ينعكس سلبا على تلقى البنك الإلكتروني للخدمة. والأصل أن هذا الالتزام في ضوء طبيعته يعد التزامًا ببذل عناية؛ باعتبار أن البنك عليه الانتفاع بالأجهزة ومتابعة هذا الانتفاع مادام متعهد الإيواء واضعا هذه الأجهزة تحت تصرفه. فمتعهد الإيواء يجب عليه بذل عناية الرجل المعتاد في ذات ظروفه ليضمن استمرار انتفاع البنك بخدماته طوال مدة العقد.

ج – يلتزم متعهد الإيواء باعتباره مخزن ومستودع الموقع الإلكتروني للبنك في البيئة الافتراضية، بالحفاظ على سرية كل البيانات التي يتضمنها الموقع، وذلك ضد كل محاولات الاطلاع غير المشروع عليها[٢]، سواء تعلقت هذه البيانات

---

(1) **Ibid**: p. 28.

(٢) وغالبا ما يلجأ متعهد الإيواء في سبيل تحقيق هذا الهدف إلى تحصين الموقع من خلال

بالبنك (كالبيانات التي تحتويها قاعدة بيانات البنك)، أو بعملائه أثناء تعاملهم مع الموقع، ويلتزم متعهد الإيواء بالحفاظ على سلامة هذه البيانات، وذلك ضد كل محاولات تعديل أو تحريف أي بيانات خاصة بالموقع، وألا يسمح لأحد بالاطلاع على هذه البيانات إلا في الحالات التي يسمح فيها القانون بذلك(١). ويجب على البنك الإلكتروني أن يشدد من مسؤولية متعهد الإيواء في هذا الخصوص، بأن ينص في العقد المبرم بينهما على أن هذا الالتزام التزام بتحقيق نتيجة، بحيث يكون الخطأ مفترضًا في جانب متعهد الإيواء بمجرد حدوث انتهاك لسرية البيانات أو سلامتها التي يتضمنها موقع البنك، ولا يستطيع متعهد الإيواء في هذه الحالة دفع مسؤوليته إلا بإثبات السبب الأجنبي.

ويبرر التشديد من مسؤولية متعهد الإيواء بخصوص الالتزام بسرية وسلامة

الاعتماد على بعض البروتوكولات التي تحقق له ذلك مثل بروتوكول الهوية (Host Identity Protocol)، حيث يعمل هذا البروتوكول على تأمين عمليات الاتصال بالموقع والتعامل معه من خلال وضع نظام مشفر للتعرف على طبيعة رسائل البيانات القادمة للموقع، انظر :

Richard H. Paine, Op., Cit, Pages 85-89.

(١) وقد ورد النص صراحة على هذا الالتزام في كثير من عقود تقديم خدمات الإيواء:

1. Datarealm will not sell or knowingly disclose its customer lists or customer email or listserv address lists. We will attempt to protect the privacy of our customers and their information that is stored on our network. Datarealm will only access and disclose information as necessary to comply with applicable laws and government requests, to Operate and maintain our systems and services, or to protect ourselves or our customers.
2. Datarealm will not monitor or disclose a customer's private email messages unless required by court order or law. We will coOperate with the authorities and will notify such authorities if it suspects that a customer is engaged in illegal activities.

البيانات التي يشتمل عليها موقع البنك بأنه أكثر مقدمي الخدمات الإلكترونية اللازمة لتشغيل البنك الإلكتروني على شبكة الإنترنت اطلاعا على المعلومات التي يتضمنها الموقع الإلكتروني للبنك، وذلك بحكم الاستضافة والإيواء، وبحكم استعمال البنك لأدواته في التعامل مع موقعه عبر شبكة الإنترنت. وقد دفع هذا الوضع القانوني لمتعهد الإيواء بعض التشريعات إلى أن تفرض عليه التزاما بالرقابة والتحكم في محتوى ومضمون ما يعرض على المواقع التي يستضيفونها(١). وقد أكدت هذا المعنى أيضا أحكام قضائية عديدة، والتي تبنت لإقامة مسؤولية متعهد الإيواء فكرة وجود نوع من الرقابة التوجيهية لمتعهد الإيواء على ما يعرض في المواقع المستضافة(٢).

---

(١) كقانون المعايير الصينية لإدارة خدمات المعلومات على شبكة الانترنت الصادر ٢٠٠١ (Chinese Measures on the Administration of internet Information Services 2001)، والقانون الصيني لإدارة النشر على شبكة الانترنت الصادر2002 (Chinese Internet Regulations on the Administration of Internet publishing).

Chris Reed; Op., Cit, p. 95.

(٢) وهذا ما أخذ به القضاء الإيطالي عندما ذهبت محكمة روما في أحد أحكامها إلى "أن طبيعة عمل متعهد الإيواء تفرض عليه أن يمارس نوعا من الرقابة التوجيهية على محتوى المواقع الإلكترونية التي يؤويها، وتلزمه في حالة العلم بعدم مشروعية المحتوى التوقف عن إيواء الموقع، وسحب المحتوى غير المشروع كلما تمكن من ذلك". انظر تفصيل ذلك د. **شريف محمد غنام**، المرجع السابق، ١٧٦، وما بعدها.

- ذهب القضاء الفرنسي أيضا في أحد القضايا التي رفعت ضد شركة Yahoo بصفتها مستضيفة لأحد مواقع المزاد (auction site) التي تعرض لبيع مواد تذكارية نازية (neo Nazi materials) بالمخالفة لقوانين مناهضة النازية (French anti-Nazi laws)، حيث ذهبت المحكمة إلى مسؤولية شركة Yahoo عما حدث، وأمرت بإلزامها بمنع الدخول إلى هذا الموقع.

Chris Reed, Op. Cit; p. 95.

Online liability decision stands, Editor& Publisher. 1/13/96, Vol.

وفي الاتجاه ذاته تسير بعض آراء الفقه التي ترى أن القائمين بالتسكين يقع عليهم التزام بالتدخل لمنع بث المحتوى غير المشروع للمواقع التي يقومون بتسكينها، ويعللون لذلك بأنهم ليسوا مجرد وسطاء فنيين، ولكنهم مسئولون عن محتوى الرسائل التي تبث عبر الموقع المستضاف، بحكم ما لديهم من أجهزة يستطيعون من خلالها الرقابة والتحكم في هذه الرسائل[1].

٨١- وعلى الرغم من تسليمنا بما أكدته التشريعات وأحكام القضاء، وآراء الفقه سالفة الذكر في خصوص التزام متعهد الإيواء بممارسة نوع من الرقابة، بحكم الدور الذي يلعبه في استضافة الموقع، إلا أن القول بذلك لا يكون على إطلاقه، فيجب على متعهد الإيواء أن يربط حجم الرقابة بطبيعة الموقع المستضاف، ونوعية الخدمات التي يقدمها هذا الموقع. فالموقع الذي يقوم بعرض مقالات أو إعلانات أو صور يمكن القول معه بضرورة ممارسة متعهد الإيواء لنوع من الرقابة على محتوياته، بالنظر إلى طبيعة خدمات هذا الموقع وما قد يحتويه من أمور تقتضي الرقابة، الأمر الذي لا يظهر بذات الأهمية في حالة استضافة موقع البنك الإلكتروني، وذلك لسببين:

الأول: طبيعة الخدمات التي يقدمها البنك على شبكة الإنترنت، وهي الخدمات المصرفية، والتي تقتضي بحكم طبيعتها عدم الاطلاع عليها إلا من قبل أطرافها المختصين فقط. فالبنك يكون حريصا دائما على إحاطة تعاملاته بسياج منيع من

129, p. 1, Academic Search Premier.

(1) **Francillon**, Infractions relevant du droit de l'information et de la communication, Rev. sc. crim, juill. 1999. p. 61.

مشار إليه لدى د. **شيماء عبد الغنى محمد عطا الله**، الحماية الجنائية للمعاملات الإلكترونية، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، ٢٠٠٥، ص٢٠٦

السرية، الأمر الذي يجعله يحول دون وجود رقابة أو متابعة لنشاطه إلا في أضيق الحدود.

الثاني: أن البنك الإلكتروني، قبل ممارسة عمله الفعلي على شبكة الإنترنت، يحتاج إلى ترخيص بذلك من البنك المركزي، حيث يعمل الأخير على التأكد من توافر الشروط الخاصة بممارسة العمل المصرفي، كما يظل يمارس نوعا من الرقابة على عمل هذا البنك، الأمر الذي يقلل من أهمية رقابة متعهد الإيواء على مضمون الموقع.

وقد دعم موقفنا التوجيه الأوربي (EC/2000/31) وذلك في المادة (١٥) منه حيث ذهب إلى منع فرض التزام على متعهد الإيواء بمراقبة المعلومات الموجودة على الموقع الذي يقوم باستضافته(١).

ويبدو لنا أن هذا التوجيه يخفى الرغبة في الحد من سلطة متعهد الإيواء في التدخل أو الاطلاع على المحتوى المعلوماتي للموقع المستضاف لديه.

لكن على الرغم من كل ذلك يبقى متعهد الإيواء ملتزما بالسرية المصرفية(٢) لما قد يصل إلى علمه من بيانات حتى ولو عن طريق المصادفة. وبناء عليه يجب على البنك أن يرسم حدودا فاصلة لدور متعهد الإيواء في التعامل مع موقعه، وذلك من خلال تحديد الأماكن التي يمكن له الدخول عليها من خلال

---

(١) وقد برر هذا التوجيه ذلك بأنه يصعب على متعهد الإيواء القيام بمهام الرقابة على محتوى الموقع المستضاف، من الناحيتين العملية والاقتصادية. انظر:

Mark Turner and Mary Traynor; Op. Cit, p. 115.

(٢) ويسرى على متعهد الإيواء ما يسرى على مصمم الموقع من التزام بالمحافظة على السرية المصرفية. انظر سابقا، ص ١٧٢.

الموقع على نحو يكفل له السرية التامة لكل ما يتم على الموقع سواء من صفقات تبرم من خلال هذا الموقع، أم من رسائل تتم عبر البريد الإلكتروني للبنك(١).

٢)- التزامات البنك الإلكتروني في مواجهة متعهد الإيواء:

٨٢- تتعدد الالتزامات الواقعة على عاتق البنك الإلكتروني في مواجهة متعهد الإيواء على النحو التالي:

أ) يلتزم البنك الإلكتروني بدفع مقابل دوري، وذلك وفق ما سيتم الاتفاق عليه مع متعهد الإيواء. ويجب على البنك أن يراعى أداء المبلغ في المواعيد المتفق عليها، وبالطريقة المتفق عليها (والتي غالبا ما ستكون بالدفع الإلكتروني عبر شبكة الإنترنت) وبصورة منتظمة، حتى يتجنب البنك قيام متعهد الإيواء بقطع الخدمة، دون الرجوع للبنك في ذلك. إذ غالبا ما تتضمن عقود تقديم خدمة الإيواء إعطاء متعهد الإيواء الحق في إنهاء العقد بالإرادة المنفردة في مثل

(١) ونظرا لأهمية السرية في التعاملات الإلكترونية بصورة عامة، والبنوك الإلكترونية العاملة عبر شبكة الانترنت بصورة خاصة، والتي تعد وبحق من أهم الأمور التي تشغل بال المتعاملين عبر هذه الشبكة، فقد قامت بعض الحكومات في بعض الدول مثل روسيا في إحكام قبضتها إلى حد ما على كثير من الجرائم التي تقع عبر هذه الشبكة، والتي تستهدف في معظمها السرية، وذلك من خلال ممارسة نوع من الرقابة على البريد الإلكتروني وكافة أشكال النقل الإلكتروني الأخرى سواء في مواجهة المستخدمين (users) أم مقدمي الخدمات الإلكترونية (Internet Service Providers). هذا على الرغم من أن الولايات المتحدة الأمريكية اعتبرت أن أية ولاية تقوم بذلك فهي تعتدي على الحقوق الدستورية للأمريكيين. وقد اشترط مكتب التحقيق الفيدرالي (FBI) لممارسة مثل هذا الإجراء ضرورة الحصول على إذن قضائي، وأن تمارس الرقابة في حدود ضيقة.

Roger Gerleroy Miler – Gaylord A. Jentz, Op., Cit. p. 14.

هذه الحالة وبدون سابق إنذار[١]. ويبرر هذا الموقف طبيعة الأداءات المتبادلة بموجب العقد المبرم بينهم؛ فالخدمة تقدم من متعهد الإيواء نظير قيام البنك بأداء المقابل المالي لذلك، ومن ثم إذا تخلف البنك عن التزامه، كان متعهد الإيواء في حل من التزامه أيضا.

ومع تسليمنا بذلك نميل إلى القول بأن يلتزم متعهد الإيواء، قبل قطع الخدمة، ضرورة توجيه إنذار للبنك، بحيث إذا تخلف البنك على الرغم من ذلك، فلا حرج على متعهد الإيواء بقطع الخدمة في هذه الحالة. ونبرر هذا الرأي بأن طبيعة عمل البنك الإلكتروني كمؤسسة تؤدى خدمات ذات أهمية كبيرة، سواء بالنسبة للعملاء، أو بالنسبة للاقتصاد القومي في مجموعه تقتضى منا الحرص على تواصل تقديم الخدمة وعدم التسرع في قطعها بدون سابق إنذار، خاصة أن خدمة الإيواء أو الاستضافة في حياة البنك الإلكتروني العامل عبر شبكة الإنترنت تحظ بأهمية كبيرة، الأمر الذي يجب معه على البنك أن يحرص على تأمين تواصل تقديم مثل هذه الخدمات في مختلف الظروف.

ب) يلتزم البنك الإلكتروني باستعمال أجهزة متعهد الإيواء بطريقة تتفق مع مقتضيات حسن النية في الاستعمال. فالبنك مجرد منتفع بهذه الأجهزة، وهو مطالب بردها عند انتهاء العقد لأي سبب، ومن ثم يجب عليه أن يستعملها بطريقة جيدة، وأن يبلغ متعهد الإيواء بأي عطل يصيب هذه الأجهزة فور حدوثه، وأن يتابع صيانة هذه الأجهزة. ونميل إلى القول بأن البنك

---

(١) راجع:
Web Hosting Agreement, available at: http://www.metrOpark.com/internet_pricing/WebHosting_Agreement.pdf

الإلكتروني، في مثل هذا الالتزام، مكلف فقط ببذل عناية. والسبب في ذلك هي قلة الخبرة الفنية بالنسبة للبنك في إدراك مثل هذه الأمور والتواصل معها، ومن ثم يقاس مقدار العناية والحرص الواجب اتباعهما من البنك بمعيار الشخص العادي في نفس ظروف البنك الإلكتروني.

ج) يلتزم البنك الإلكتروني في مواجهة متعهد الإيواء بمراعاة الضوابط الأخلاقية والقانونية في كل ما يقوم بعرضه على الموقع الإلكتروني الخاص به على شبكة الإنترنت، فلا يقوم مثلا بعرض أي صور أو مقالات إباحية، أو عرض أمور تحض على ارتكاب الجرائم، أو يقوم بعرض أي عمل يشكل انتهاكا لحقوق الملكية الفكرية الخاصة بأي شخص آخر، مثل تداول برامج معلوماتية بصورة غير قانونية، حيث يكون مسئولا عن أي فعل يشكل انتهاكا لذلك(١)، وغالبا ما تنص عقود تقديم خدمات الإيواء على إعطاء متعهد الإيواء سلطة إنهاء العقد بالإرادة المنفردة في حالة وجود مثل هذه الأمور، وحتى دون الرجوع للعميل (البنك الإلكتروني)(٢). كما ينص أيضا على إعفائه من كل مسؤولية في حالة قيام العميل (البنك الإلكتروني) بأى عمل يتنافى من الضوابط الأخلاقية والقانونية سالفة الذكر.

ونحن من جانبنا نؤكد على حق متعهد الإيواء في قطع الخدمة في مثل هذه الحالات، فمادام الأمر قد وصل إلى حد الاعتداء على الضوابط الأخلاقية

---

(1) **E-Banking,** Federal Financial Institutions Examination Council; Op. Cit., p. 4.

(2) **HiTeach,** web hosting contract, available at: http://www.hitech-solutions.com /Contract_hosting.asp; **Website hosting contract and terms of service agreement,** Op. cit.

والقانونية، فيجب على متعهد الإيواء في مثل هذه الحالة أن يحول دون عرض مثل هذه الأمور، وإلا كان مسئولا.

- مسؤولية الأطراف المتعاقدة:

يمكن أن تثور مسؤولية كل من متعهد الإيواء والبنك الإلكتروني، في ضوء الالتزامات السابقة، وذلك على النحو التالي:

١)- مسؤولية متعهد الإيواء فى مواجهة البنك:

تعرفنا فيما سبق على طبيعة الالتزامات الملقاة على عاتق متعهد الإيواء بموجب عقد الإيواء، والتي عكست الدور بالغ الأهمية الذي يطلع إليه بحكم استضافته لموقع البنك على الانترنت، وذلك على النحو الذي يثير التساؤل حول طبيعة مسؤوليته الجنائية والمدنية عن مخالفة هذه الالتزامات، وذلك على النحو التالي:

(أ) المسؤولية الجنائية لمتعهد الإيواء فى مواجهة البنك:

٨٣- يمكن أن تجد المسؤولية الجنائية لمتعهد الإيواء سبيلها إذا أخل بالالتزام المفروض عليه بالحفاظ على سرية وسلامة البيانات التي يطلع عليها بسبب طبيعة عمله (ويتشابه دور متعهد الإيواء في هذا الخصوص مع دور مصمم موقع البنك الإلكتروني)، بموجب نص المادة ٣٠٩ من قانون العقوبات المصري (سالفة الذكر)، والتي نصت على أن 'يعاقب بالحبس مدة لا تزيد على سنة كل من استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه، ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما

يكون قد استخدم في الجريمة، كما يحكم بمحو التسجيلات المتحصلة عنها أو إعدامها". فطبيعة عمل متعهد الإيواء كمستضيف للموقع الإلكتروني للبنك على الأجهزة الخاصة به تتيح له الفرصة عن قصد أو بدون قصد للاطلاع على البيانات الخاصة بالبنك (خاصة قاعدة البيانات الخاصة بالبنك)، الأمر الذي يجعله مسئولاً جنائيا بموجب النص السابق.

أيضا يمكن أن يسأل متعهد الإيواء جنائيا عن أي انتهاك قام به لأي من الأشياء الموجودة على موقع البنك، والتي يحميها القانون باعتبارها من عناصر الملكية الفكرية، فقيام متعهد الإيواء بحكم استضافته لموقع البنك بالاعتداء، أو بتسهيل الاعتداء على أي تصميم أو صورة أو اسم أو علامة تجارية، بالتقليد أو المحاكاة أو التغيير أو التحريف، مع توافر القصد الجنائي لذلك يجعله مسئولاً جنائيا عن ذلك.

فقد نص قانون الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢ الخاص بحماية الملكية الفكرية في المادة ١١٣ منه على أنه "مع عدم الإخلال بأي عقوبة أشد في أي قانون آخر يعاقب بالحبس مدة لا تقل عن شهرين وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين:....

كل من زور علامة تجارية تم تسجيلها طبقا للقانون أو قلدها بطريقة تدعو إلى تضليل الجمهور".

وقد ورد في ذات القانون، وتحديدا نص المادة ١٨١ أنه "مع عدم الإخلال بأي عقوبة أشد في قانون آخر يعاقب بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرة آلاف جنيه، أو بإحدى هاتين العقوبتين، كل من ارتكب أحد الأفعال الآتية:

- بيع أو تسجيل مصنف أو تسجيل صوتي أو برنامج إذاعي محمى طبقا لأحكام هذا القانون، أو طرحه للتداول بأي صورة بدون إذن كتابي مسبق من المؤلف أو صاحب الحق المجاور.

- تقليد مصنف أو تسجيل صوتي أو برنامج إذاعي أو بيعه أو طرحه للتداول أو للإيجار مع العلم بتقليده.

- التقليد في الداخل لمصنف أو تسجيل صوتي أو برنامج إذاعي أو أداء محمى طبقا لأحكام هذا القانون عبر أجهزة الحاسب الآلي أو شبكات الإنترنت أو شبكات المعلومات أو شبكات الاتصالات أو غيرها من الوسائل بدون إذن كتابي مسبق من المؤلف أو صاحب الحق المجاور.

- التصنيع أو التجميع أو الاستيراد بغرض البيع أو التأجير لأي جهاز أو وسيلة أو أداة مصممة أو معدة للتحايل على حماية تقنية، يستخدمها المؤلف أو صاحب الحق المجاور كالتشفير أو غيره.

- الاعتداء على أي حق أدبي أو مالي من حقوق المؤلف أو الحقوق المجاورة المنصوص عليها في هذا القانون.

وعلى الرغم من اعتناق النصوص السابقة لعبارات عامة قادرة على استيعاب الانتهاكات التي يمكن أن تقع من قبل متعهد الإيواء على موقع البنك الإلكتروني، إلا أن هذه النصوص لا تقدم من وجهة نظرنا إلا مجرد علاج مؤقت لمشكلة جد خطيرة، الأمر الذي يحتاج إلى معاملة عقابية خاصة لمتعهد الإيواء وذلك لسببين:.

الأول: طبيعة عمل متعهد الإيواء كأمين على الموقع الإلكتروني للبنك ومستودع

لحفظه، الأمر الذي يدفع إلى القول بمعاملة عقابية متشددة لأي انتهاك قـام بـه بنفسه أو سهل القيام به، وذلك من خلال تغليظ العقوبة مثلا، أو إضافة عقوبـات إلى العقوبات الموجودة، كوقف الترخيص الذي يسمح له بممارسة عمله.

الثاني: الطبيعة الخاصة جدا للموقع المستضاف، وهو موقع البنك الإلكتروني، حيث تبدو هذه الخصوصية وتتجلى من خلال النظر إلى طبيعة العمليات التي تتم عبر هذا الموقع، ومدى تأثيرًاها المباشر على مجريات التجارة الإلكترونية على شبكة الإنترنت، حيث يمثل وبحق عصب هذه التجارة، وقلبها النـابض، الأمـر الذي يدفعنا إلى أن نهيب بالمشرع المصري إلى ضرورة تبنى معاملـة عقابيـة خاصة لكافة صور الانتهاكات التي تسعى للنيل من موقع البنـك الإلكترونـي، خاصة الانتهاكات التي تنال من وجود هذا الموقع على شبكة الإنترنت، كـالتي تسعى لتقليد علامته التجارية أو عنوانه الإلكتروني أو اسمه التجاري.

وما أحسن ما فعله المشرع الأمريكي في هذا الصدد، حيث راعى الطبيعـة الخاصة لعناصر الملكية الفكرية الموجودة على شبكة الإنترنت، وأصدر في عام ١٩٩٧ قانونًا خاصًا بالسرقة الإلكترونيـة (No Electronic Theft Act) (١)، وسع من خلاله المسؤولية الجنائية للمعتدى علـى عناصـر الملكيـة الفكريـة الموجودة على شبكة الإنترنت، حيث لم يكتف بتجريم الاستخدام غير المـشروع لهذه العناصر، بل جرم التبادل غير المرخص به لهذه العناصر حتى لو لم يكـن بقصد الاتجار والحصول على الربح من ورائها، بل وصل به الحال إلى تجريم

---

(1) Available at: http://www.ipmall.info/hosted_resources/lipa/copyrights/NoElectronicTh eftNE TActPublicLaw105147.pdf

إعادة نسخ أي من هذه العناصر حتى لو للاستعمال الشخصي(١).

لكن هل يمكن أن يسأل متعهد الإيواء عن أي انتهاك يقع من الغير على أحد عناصر الملكية الفكرية، وذلك باعتباره المسئول عن استضافة الموقع وتخزين محتوياته على الأجهزة الخاصة به؟

لقد أجاب التوجيه الأوربي رقم (٢٠٠٣/٣١) في المادة (١٣) على هذا السؤال صراحة وذلك بإعفاء متعهد الإيواء من المسؤولية عن أي اعتداء يقع من الغير على أي شيء موجود على موقع البنك ومشمول بالحماية كأحد عناصر الملكية الفكرية أو الصناعية. وقد برر هذا التوجيه هذا الإعفاء بالدور الفني البحت لمتعهد الإيواء. وقد عبر عن ذلك بأنه مجرد قناة (mere conduits) لمحتوى الموقع. غير أنه قد وضع عدة شروط للاستفادة من هذا الإعفاء من المسؤولية، تتمثل في(٢):

- ألا يكون متعهد الإيواء قد قام بتعديل أو تغيير محتوى أحد هذه العناصر.
- أن يكون متعهد الإيواء قد قام باتخاذ كافة الإجراءات اللازمة لإزالة وتعطيل وصول أي شخص أجنبي لمصدر العناصر المحمية.
- ألا يكون قد قام باعتراض أي استخدام قانوني لأحد هذه العناصر.

---

(1) **Roger Gerleroy Miler – Gaylord A. Jentz**, Law; Op. Cit; P. 119.

(2) **Stephen Rawson, Partner, Denton Wilde Sapte,** Op. Cit. p. 168; **Holland, Bill, Billboard**. U.S.' Wipo bill is entwined with online liability issue, 00062510, 09/27/97, Vol. 109. Billboard Journal.available at: http://www.allbusiness.com/retail-trade/ miscellaneous-retail-retail-stores-not/4661925-1.html

- أن يكون قد التزم بكافة التعليمات التي وضعها صاحب أحد هذه العناصر فيما يتعلق بالدخول عليها أو تعديل محتواها.

وقد كان هذا هو موقف التوجيه الأوربي الخاص بحماية الملكية الفكرية، حيث قرر إعفاء متعهد الإيواء من المسؤولية عن هذه الانتهاكات أيضا(١).

أما عن موقف القانون الأمريكي في هذا الخصوص، فإننا نلاحظ أن قانون الملكية الفكرية ظل فترة طويلة ملتزما الصمت تجاه مسؤولية متعهد الإيواء عن الانتهاكات التي تقع من الغير على عناصر الملكية الفكرية الموجودة على الموقع المستضاف(٢). لكن يبدو أن هذا الوضع لم يكن يروق المحاكم الأمريكية، حيث رفعت راية العصيان على هذا الصمت التشريعي، وذهبت إلى إمكانية انعقاد مسؤولية متعهد الإيواء في هذا الفرض(٣)، وذلك في حالة توافر شرطين(٤):

الأول: وهو توافر علاقة بين متعهد الإيواء ومن قام بالانتهاك.

---

(1) **Mark Owen, Richard Penfold**, Copyright infringement in the online world, Dec99/ Jan 2000, Issue 95, Database, Academic Search Premier.

(٢) حيث تم تعديل قانون الملكية الفكرية بعد ذلك وتبنى ما استقر عليه القضاء في هذا الخصوص. انظر

Mark Turner and Mary Traynor, Herbert Smith, Op, Cit, p. 117.

(٣) وقد أطلقت المحاكم الأمريكية على هذه المسؤولية عبارة المسؤولية البديلة **(Vicarious_liability)**.

(4) **Bryan Mercurio BA (Hons)**, Internet service provider Liability for copyright infringements of subscribers, E law- Murdoch University- Electronic journal of law, Vol. 9, Number 4, December 2002, p 3; **Michael D. Scott**; Op. Cit., p. 452.

الثاني: أن يكون متعهد الإيواء قد استفاد ماليا من وراء عملية الانتهاك.

وعن الشرط الأول، يبدو أن القضاء الأمريكي يتطلب وجـود نـوع مـن التدخل من قبل متعهد الإيواء، وذلك من خلال المساعدة أو الاتفاق بينه وبين من يقوم بالانتهاك كشرط لمسؤولية متعهد الإيواء. وهذا يعد أمر طبيعيا ومفترضـا حيث لا مجال للحديث عن المسؤولية الجنائية لمتعهد الإيواء إن لم يكـن هنـاك تدخل من جانبه أيا كانت صورة هذا التدخل، حتى يسأل في هذه الحالة (إعمـالا لمبدأ شخصية العقوبة). وعن الشرط الثاني فأنه يعكس نظرة القضاء لهذا الفعل؛ وأنه لا يكتفي لتحقق الانتهاك مجرد وقوع الاعتداء على أحد العناصر المحمية. بل يلزم لذلك أيضا تحقق نتيجة معينة، وهي الاستفادة الماليـة مـن وراء هـذا الانتهاك.

ويبدو لنا أن القضاء الأمريكي قد حالفه الصواب فيما يخص الشرط الأول. أما الشرط الثاني فقد كان مدخلا لتوجيه سهام النقد إليه، حيث كان من الواجـب عليه أن يكتفي بمجرد وقوع الاعتداء على أحد العناصر المحمية، بسبب العلاقة التي تربط بين متعهد الإيواء والشخص المعتدى دون الانتظار إلى حد اسـتفادة متعهد الإيواء ماليا من هذا الاعتداء. ويبدو لنا أن هذه الجـرائم هـي جـرائم نشاط[١]، أي أن الضرر يتحقق فيها لمجرد ممارسة النشاط المتمثل في الاعتداء على أحد هذه العناصر، دون الاعتداد بتحقق استفادة مالية من عدمه.

(١) وتعرف جريمة النشاط بأنها عبارة عن جريمة يتألف ركنها المادي من مجرد سـلوك إجرامي كاف وحده لتحقيق النتيجة في معناها القانوني أو الاعتداء علـى المـصلحة المحمية. ويطلق عليها جرائم الخطر، وهي مثل إحراز المخدرات، حمل سلاك بدون ترخيص. انظر. د. **أحمد شوقي أبو خطوة**، الأحكام العامة لقانون العقوبات، النظرية العامة للجريمة (الجزء الأول)، دار النهضة العربية، ١٩٩٩، ص ١٩١.

ويتضح من خلال استعراض موقف كل من التوجيه الأوربي والقضاء الأمريكي أنه لا يوجد تباين كبير بينهما، حيث إن الأول وأن جعل الإعفاء من المسؤولية هو الأصل، لكنه ربط ذلك بشروط معينة بحيث إذا أختل أحد هذه الشروط قامت المسؤولية. أما الثاني فقد اعترف بالمسؤولية وجعلها الأصل في الحكم على موقف متعهد الإيواء. ويبدو لنا على الرغم من ذلك رجحان موقف القضاء الأمريكي في هذا الخصوص، من حيث أنه جعل الأصل هو مسؤولية متعهد الإيواء عن الاعتداءات التي تقع من الغير على أحد محتويات موقع البنك والمشمولة بالحماية كأحد عناصر الملكية الفكرية أو الصناعية، وترجع العلة من هذا الترجيح في أهمية وخطورة هذه العناصر، فالاسم التجاري، والعلامة التجارية، والعنوان الإلكتروني، والتصميمات الخاصة بموقع البنك الإلكتروني، وغيرها من الأشياء التي تميز البنك وتميز خدماته، تزداد أهميتها عندما يكون كيان البنك ومنفذ خدماته على شبكة الإنترنت. وعندما يرغب عميل البنك في الوصول إليه على شبكة الإنترنت لن يجد أمامه مرشدا ودليلا يأخذ بيده إلا هذه العناصر، الأمر الذي يبرر التشدد في حمايتها، وذلك من خلال إشراك متعهد الإيواء في المسؤولية عن أية انتهاكات ترد عليها.

(ب) المسؤولية المدنية لمتعهد الإيواء فى مواجهة البنك:

٨٤- يسأل متعهد الإيواء مدنيا عن أي إخلال يقع من جانبه بأحد الالتزامات الواردة في عقد الإيواء، وذلك في مواجهة البنك الإلكتروني سواء تمثل هذا الإخلال في عدم تنفيذ الالتزام أصلا، أم تنفيذه بصورة غير مطابقة (على نحو

سيء أو في وقت متأخر)[1]. ويتحدد إخلال متعهد الإيواء بحسب طبيعة كل التزام عقدي؛ فإذا كان التزام متعهد الإيواء التزاما بتحقيق نتيجة(كالتزامه بتمكين البنك الإلكتروني من الانتفاع بأجهزته وبرامجه)، فإن متعهد الإيواء يسأل في حالة عدم تحقق هذه النتيجة، ولا يلزم البنك الإلكتروني في هذه الحالة أن يثبت خطأ متعهد الإيواء، بل يكفيه إثبات عدم تحقق النتيجة المتفق عليها. ولا يستطيع متعهد الإيواء أن يدفع مسؤوليته إلا بإثبات السبب الأجنبي. أما إذا كان التزام متعهد الإيواء التزاما ببذل عناية (كالتزامه بمتابعة استمرار انتفاع البنك بخدماته)، فإنه يكفيه أن يبذل عناية الشخص المعتاد في ذات ظروفه، بحيث تنعقد مسؤوليته في حالة ثبوت عدم بذله العناية المطلوبة في تنفيذه لالتزامه على نحو ألحق ضررا بالبنك الإلكتروني. ويجب على البنك أن يثبت تقصير متعهد الإيواء في بذله للعناية المطلوبة حتى تقوم مسؤوليته.

والملاحظ على عقود تقديم الخدمات الإلكترونية بصورة عامة أن الشركات القائمة على تقديم هذه الخدمات تقوم بإعداد هذه العقود في صورة عقود نموذجية، تتضمن تعديلاً من قواعد مسؤوليتها العقدية (كجعل التزام بتحقيق نتيجة التزاما ببذل عناية، وذلك حتى تلقى بعبء إثبات المسؤولية على عاتق الدائن)، أو الإعفاء من هذه المسؤولية تماما (المسؤولية العقدية) باعتبار أن القواعد التي تحكم تنظيم هذه المسؤولية تتيح ذلك، مادام الأمر لا يتعلق بالغش أو الخطأ الجسيم[2].

---

(١) **د. محمد عبد الظاهر حسين**، المسؤولية القانونية في مجال شبكات الانترنت، المرجع السابق، ص ٧.

(٢) **د. محمد حسين منصور**، مرجع سابق، ص٩١

وهنا يجب على البنك الإلكتروني أن يتسلح بسلاح الحذر في مواجهة مثل هذه الشروط والبنود المصوغة بعبارات مجملة وعامة، والتي تستهدف في النهاية التخفيف من مسؤولية مقدم الخدمة أو الإعفاء منها، على نحو يجعل هذه الشروط شروطا تعسفية(1)، قابلة للتعديل أو الإعفاء منها من قبل القضاء(2). وبناء عليه يجب على البنك ألا يلقى بنفسه في فلك هذا العقود ويدور معها أينما دارت، بل يجب عليه توخي الحيطة والحرص الشديدين من توافر نصوص صارمة تكفل

---

(1) ويعرف **الشرط التعسفي** بأنه عبارة عن اشتراط مفروض بواسطة مقدم الخدمة أو السلعة بهدف الحصول على وضع مميز في مواجهة المستهلك، وعلى نحو يؤدى إلى الإضرار بمصالحه بسبب عدم التوازن الواضح بين حقوق والتزامات مقدم السلعة أو الخدمة والمستهلك وذلك في أي مرحلة من مراحل التعاقد. **د. خالد ممدوح إبراهيم**، حماية المستهلك في المعاملات الإلكترونية، الدار الجامعية، ٢٠٠٧، ص ١٩٤ وما بعدها.

Unfair terms - some terms are made unfair by legislation and will not be enforced by the courts and may even be interpreted against the person who included them in the contract. The legislation mainly protects consumers, but can also apply where there is a business-to-business contract in which one party is significantly more powerful than the other Business contracts legal terms and definitions glossary, business balls, available at: http://www.businessballs.com/businesscontractstermsdefinitions glossary. htm.

(2) **تنص المادة ١٤٩ من القانون المدني المصري** على أنه "إذا تم العقد بطريق الإذعان، وكان قد تضمن شروطا تعسفية، جاز للقاضي أن يعدل هذه الشروط أو أن يعفى الطرف المذعن منها، وذلك وفقا لما تقضى به العدالة ويقع باطلا كل اتفاق على خلاف ذلك".

- ويذهب بعض الفقه بحق إلى القول بأن هذا النص يمنح القاضي سلطة غير عادية في تعديل الشروط التعسفية أو الإعفاء منها، وفقا لما تقضى به العدالة من غير تخصيص ولا تمييز بين هذه الشروط، سواء علم بها الطرف المذعن أم لم يعلم. **د. محسن عبد الحميد البيه**، مرجع سابق، ص ١٩٣، انظر أيضا: **د. أسامة أحمد بدر**، مرجع سابق، ص ١٩٢.

حدا معقولا من المسؤولية، وذلك حتى يضمن لنفسه أقصى مستوى من الخدمة، في ظل بيئة إلكترونية يجهل فيها البنك بحكم طبيعة عمله المصرفي الخبرة الفنية.

لكن هل يمكن القول بأن اعتماد مقدمي الخدمات الإلكترونية- عبر شبكة الإنترنت- العقود النموذجية كوسيلة للتعاقد مع البنك الإلكتروني أم أن عقودهم هذه تعد عقود إذعان؟

٨٥- يعرف عقد الإذعان بأنه عبارة عن عقد ينفرد أحد الأطراف فيه بوضع شروطه وفرضها على الطرف الآخر الذي لا يملك مناقشتها، وذلك بخصوص سلع أو خدمات ضرورية تكون محل احتكار قانوني أو فعلي(١).

ويعرف العقد النموذجي Contract type بأنه عبارة عن عقد معد مسبقا من قبل أحد أطراف التعاقد(٢) بصيغة معينة تتضمن تنظيم التعاقد، وغير قابلة للمناقشة من قبل المتعاقد(٣).

ويتضح من خلال هذان التعريفين أن كل عقد نموذجي ليس بالضرورة عقد إذعان.

---

(١) د. **عبد المنعم فرج الصدة**، عقد الإذعان، مجلة الأمن والقانون، كلية شرطة دبي، السنة الرابعة،العدد الأول، ١٤١٦- ١٩٩٦، ص٢٤٣؛ د. **محسن عبد الحميد البيه**، المرجع السابق، ص ١٧٣.

(٢) وغالبا ما تصاغ هذه العقود من قبل سلطات عامة أو منظمات مهنية، وذلك بهدف وضع تنظيم مفصل للقواعد والأحكام التي تحكم هذه العقود على أن يلتزم بها المتعاقدان بموجب تعهدات تصدر منهم تفيد ذلك د. **فتحي عبد الرحيم عبد الله**، الوجيز في النظرية العامة للالتزامات، مكتبة الجلاء الجديدة بالمنصورة، الطبعة الثانية، ١٩٩٩، ص ٥٣.

(3) **Michael chissick, Alistair Kelman,** Op. Cit., p. 99.

- فأوجه الشبه بين العقدين تتلخص في سبق إعداد العقد، وعدم السماح بمناقشة شروطه. في حين أن هناك وجها للاختلاف كفيلا بإحداث الفرقة بين هذين العقدين، وهو وجود احتكار قانوني أو فعلى من قبل مقدم السلعة أو الخدمة في عقد الإذعان، الأمر الذي يلوح بوجود شبهة التعسف. فالإذعان- على ما يبدو- لا يقوم بدون وجود عنصر الاحتكار في تقديم السلعة أو الخدمة، حيث أنه على فرض أن مقدم السلعة أو الخدمة يضمن العقد شروطا تعسفية، وهو ليس محتكرا لتقديم السلعة أو الخدمة، فمن السهل اللجوء إلى شخص أخر والحصّول على ذات السلعة أو الخدمة بشروط أفضل.

- اعتماد الغالبية العظمى من مقدمي السلع والخدمات على شبكة الإنترنت على العقود النموذجية كوسيلة للتعاقد أمر تبرره طبيعة التعاقد عن بعد من خلال شاشات الحاسب الإلكتروني. كما أن وجود العقد في صورة نموذجية لا يعني بالضرورة وجود شروط تعسفية فيه تبرر القول بوجود الإذعان، فقد تكون شروط العقد منطقية وتحقق التوازن بين أطرافه، على نحو تنتفي معه شبهة الإذعان في العقد.

- يضاف إلى ذلك أن وجود العقد في صورة نموذجية لا يعني عدم قابلية شروطه للمناقشة، حيث يحدث أحيانًا قيام مقدم السلعة أو الخدمة بإرسال رسالة عبر البريد الإلكتروني تتضمن إيجابا من قبله بإبرام العقد، ويرفق بهذه الرسالة عقدًا نموذجيًا معدًا سلفًا، فيقوم المرسل إليه بقبول هذا العرض، من خلال إرسال رسالة إلكترونية تتضمن الموافقة على الإيجاب المرسل إليه، والتي قد تتضمن

تعديلا من الشروط الواردة في العقد النموذجي(١)، وبعيدا عن مدى اعتبار هذا قبولا ينعقد به العقد لغياب التطابق بين الإيجاب والقبول، فإن ما يهمنا هنا هو أن العقود النموذجية يمكن أن تقبل مناقشة شروطها.

بل إن هذا ما يمكن أن يفهم مما جاء في الفقرة السابعة من التوجيه الأوربي رقم (Ec /2000/31)، والذي أوصى مقدم الخدمة بضرورة تزويد طالب الخدمة (البنك الإلكتروني) بكافة البيانات التفصيلية لعملية التعاقد على النحو الذي يجعل الأخير مؤهلا للاختيار على علم (informed choices)، وتجنيبه الدخول في صفقات تجارية غير مقصودة (unintended commercial transactions) . بل أضاف إلى ذلك في الفقرة الثامنة من ذات التوجيه ضرورة قيام مقدم الخدمة بإخبار طالب الخدمة بحقه في الرجوع في العقد خلال سبعة أيام من تاريخ انعقاده، وذلك مراعاة لكون العقد يبرم عن بعد(٢).

نخلص من كل هذا بنتيجة محددة، وهي أن اعتماد مقدم الخدمة على العقد النموذجي للتعاقد مع البنك الإلكتروني لا يعني بالضرورة وجود البنك في حالة إذعان لكن ما يجب أن يقال في هذا الصدد هو وجوب تحلى البنك الإلكتروني بالمزيد من الحرص قبل أن يلقى بنفسه في فلك أحد هذه التعاقدات ليدور معها أينما دارت، ووجوب الاستعانة بأهل الخبرة في فهم واستيعاب بنود وشروط هذه التعاقدات. وفي كافة الأحوال إذا تبين أن أحد شروط العقد من شأنها أن تثير شبهة التعسف، فيمكن أن يلجأ البنك في هذه الحالة للقضاء لإعمال نص المادة ١٤٩ من القانون المدني المصري، والتي تعطى للقاضي السلطة في تعديل العقد،

---

(١) د. خالد ممدوح إبراهيم، المرجع السابق، ص ٢١١.

(2) **Stephen Rawson, Partner, Denton Wilde Sapte,** Op. Cit., p. 164.

أو إعفاء البنك الإلكتروني من هذا الشرط.

٨٦- وتنعقد المسؤولية المدنية أيضا لمتعهد الإيواء عن كل خطأ يقع من جانبه خارج نطاق الالتزامات العقدية، يكون من شأنه أن يسبب ضررا للبنك الإلكتروني، وذلك وفقا لما تقرره المادة ١٦٣ من القانون المدني المصري. وبناء عليه إذا صدر من متعهد الإيواء أي سلوك سبب ضررا للبنك تنعقد مسؤوليته المدنية عن تعويض هذه الأضرار، بحيث إذا تمكن البنك من إثبات خطأ متعهد الإيواء، والضرر الذي لحق به، وعلاقة السببية بين هذا الخطأ وذاك الضرر. ولا يستطيع متعهد الإيواء في هذه الحالة دفع مسؤوليته إلا بقطع علاقة السببية بين الخطأ والضرر، وذلك بإثبات السبب الأجنبي.

٨٧- يسأل أيضا متعهد الإيواء في مواجهة البنك الإلكتروني عما تحدثه الأجهزة الإلكترونية الخاصة به، والتي تحدث ضررا للبنك، وذلك بموجب نص المادة ١٧٨ من القانون المدني المصري والخاصة بمسؤولية حارس الأشياء غير الحية؛ فمتعهد الإيواء يعتبر حارسا لهذه الأجهزة بموجب ما له من حراسة فعلية عليها يملك بموجبها استعمال وتوجيه والرقابة على هذه الأجهزة بصورة مستقلة، كما أن الأجهزة الإلكترونية كما سبق أن ذكرنا(١) تعد من قبيل الأشياء التي تحتاج إلى عناية خاصة بمفهوم نص المادة ١٧٨ مدني، ومن ثم يمكن للبنك أن يعود على متعهد الإيواء بوصفه حارسا عما تحدثه الأجهزة الخاصة به من أضرار. ويتميز هذا النوع من المسؤولية أن خطأ متعهد الإيواء مفترض، الأمر الذي يعفى البنك من إثبات خطأ متعهد الإيواء، ولا يملك الأخير لدفع مسؤوليته إلا أن يثبت السبب الأجنبي؛ كانقطاع مفاجئ في التيار الكهربي، أو خطأ البنك

---

(١) راجع سابقا، ص ٩٧.

في التعامل مع الأجهزة.

والسؤال ماذا لو لحق عميل البنك الإلكتروني ضرر ناجم عن الأجهزة الخاصة باستضافة الموقع الإلكتروني للبنك؟

٨٨- وفقا للمستقر عليه فقهًا وقضاءً بخصوص تحديد المقصود بالحارس في ضوء نص المادة ١٧٨ من القانون المدني، الحارس هو من له سلطة فعلية على الشيء بموجبها يملك سلطات الرقابة والتوجيه والاستعمال لحساب نفسه، ومن ثم يجب على العميل كي يقيم المسؤولية أن يثبت من هو الشخص الذي يتمتع بهذه السلطات على هذه الأجهزة البنك أم متعهد الإيواء، وذلك بصرف النظر عن لمن تكون ملكية هذه الأجهزة. فالمعول عليه من له السلطة الفعلية عليها. ولا يكلف العميل بإثبات الخطأ؛ حيث يكون الخطأ مفترضًا فيمن له السلطة الفعلية على هذه الأجهزة.

لكن هل يمكن الاكتفاء بنظم المسؤولية السابقة (العقدية، التقصيرية) لحماية البنك الإلكتروني في مواجهة الأضرار التي يمكن أن تلحق به في ظل بيئة تكنولوجية يصعب على البنك الضعيف من الناحية الفنية إثبات خطأ متعهد الإيواء؟

٨٩- تستطيع نظرية المخاطر أن تقدم للبنك الإلكتروني مزيدا من الحماية بفضل النظام القانوني الذي يحكم إعمال المسؤولية القائمة على هذه النظرية، وذلك في مواجهة الأضرار التي تلحق البنك بسبب نشاط متعهد الإيواء. فهذه النظرية تؤسس المسؤولية على عنصرين فقط هما الضرر وعلاقة السببية، دون إثارة لفكرة الخطأ، فالمسؤولية تقوم لمجرد حدوث الضرر للبنك بسبب نشاط متعهد الإيواء يستوي في ذلك أن يكون هذا النشاط خاطئا أم لا، وذلك وفقا للسلوك

المعتاد.

وقد وجه النقد لهذه النظرية، وذلك على أساس أن البنك الإلكتروني يتعذر عليه، في حالة تعدد الأسباب المؤدية للضرر، إثبات علاقة السببية. بمعنى أنه على فرض أن البنك الإلكتروني أخطأ في التعامل مع موقعه المستضاف من قبل متعهد الإيواء، كما لو لم يتبع التعليمات التي أشار متعهد الإيواء عليه بها، على نحو سبب له ضرر، فسوف تثور صعوبة في ربط هذا الضرر بنشاط أي منهما طبقا لنظرية تحمل المخاطر(١).

ويبدو لنا عدم وجود مشكلة في هذا الأمر؛ حيث لا مجال للحديث عن مسؤولية متعهد الإيواء في ظل تحقق الخطأ من قبل البنك الإلكتروني. والقول بغير ذلك هو درب من دروب الإجحاف بمتعهد الإيواء (فكما أننا حريصون أشد الحرص على تهيئة مناخ قانوني قوى للبنك الإلكتروني من خلال التشديد من مسؤولية القائمين على الخدمات الإلكترونية للبنك على شبكة الإنترنت، فيجب أن نكون حريصين أيضا على سلامة المركز القانوني لمقدم الخدمة، وعدم تحميله بأكثر مما يحتمل، حتى لا يكون ذلك مدعاة للنفور من تقديم مثل هذه الخدمات على النحو الذي يضر بالتجارة الإلكترونية في مجموعها).

فمجال الحديث عن مسؤولية متعهد الإيواء طبقا لنظرية تحمل المخاطر أنما يثور في حالة إصابة البنك الإلكتروني بضرر تسبب فيه نشاط متعهد الإيواء، حتى ولو لم يكن هذا النشاط يشكل خطأ. لكن إذا صدر عن غير متعهد الإيواء ما يشكل خطأ فهو الأولى بالمسؤولية. ويكفى أننا نحمل متعهد الإيواء المسؤولية

---

(١) **د. شريف محمد غنام**، مسؤولية البنك عن أخطاء الكمبيوتر في النقل الإلكتروني للنقود، مرجع السابق، ص ١٠٣.

عن نشاطه فقط . فلا يمكن إثقال عاتق متعهد الإيواء بالمسؤولية حتى مع تحقق خطأ البنك الإلكتروني. وبناء عليه تنحصر مسؤولية متعهد الإيواء في حالة حدوث ضرر للبنك ناتج عن استضافة موقعه لدى متعهد الإيواء، وعدم ثبوت الخطأ في جانب البنك أو غيره. يضاف إلى ذلك أنه في حالة ثبوت خطأ متعهد الإيواء، وخطأ البنك الإلكتروني، فلا مجال هنا للحديث عن نظرية تحمل المخاطر، حيث ستكون المسؤولية مؤسسة على الخطأ سواء عقديا أم تقصيريا، وسيتم في هذه الحالة البحث عن الخطأ المباشر، أو الخطأ الذي يستوعب باقي الأخطاء وتحميل فاعله المسؤولية.

ثانيًا: مسؤولية البنك الإلكتروني في مواجهة متعهد الإيواء:

في ضوء طبيعة الالتزامات الملقاة على عاتق البنك بموجب عقد الإيواء يمكن أن تثور مسؤوليته الجنائية والمدنية على التفصيل التالي:

(أ) المسؤولية الجنائية للبنك فى مواجهة متعهد الايواء:

انطلاقا من الطبيعة القانونية للعقد المبرم بين البنك الإلكتروني ومتعهد الإيواء (عقد إيجار) فإن التساؤل الذي يطفو على سطح البحث هل يمكن أن يسأل البنك الإلكتروني عن جريمة خيانة الأمانة في مواجهة متعهد الإيواء؟

٩٠- في الواقع يخلو قانون العقوبات المصري من نص خاص ينظم مسؤولية البنك الإلكتروني عن هذه الجريمة، الأمر الذي يدفعنا إلى النظر في مدى قدرة القواعد العامة على استيعاب هذا الفرض.

تنص المادة ٣٤١ من قانون العقوبات المصري على أن "كل من اختلس أو استعمل أو بدد مبالغ أو بضائع أو أمتعة أو تذاكر أو كتابات أخرى مشتملة على

تمسك أو مخالصة أو غير ذلك إضرارا بمالكيها أو أصحابها أو واضعي اليد عليها، وكانت الأشياء المذكورة لم تسلم له إلا على وجه الوديعة أو الإجارة أو على سبيل عارية الاستعمال أو الرهن أو كانت قد سلمت له بصفة كونه وكيلا بأجرة أو مجانا أو بقصد عرضها للبيع أو بيعها أو استعمالها في أمر معين لمنفعة المالك لها أو غيره يحكم عليه بالحبس ويجوز أن يزاد عليه غرامة لا تتجاوز مائة جنيه مصري".

وقبل أن نخوض في الحديث عن مدى توافر أركان جريمة خيانة الأمانة وفقا للنص السابق، نتساءل عن مدى توافر الشروط المسبقة في جريمة خيانة الأمانة، وهي:

أولا: المال المنقول، وذلك باعتباره محلا لهذه الجريمة كما عبر عن ذلك النص السابق (مبالغ أو بضائع أو أمتعة أو تذاكر أو كتابات أخرى).

ويبدو لنا أن ما يتسلمه البنك الإلكتروني من أشياء بموجب عقد الإيواء لا تخرج عن مفهوم المال المنقول وفقا للنص السابق. فتخصيص متعهد الإيواء مساحة من القرص الصلب المملوك له لاستضافة موقع البنك الإلكتروني عليه، وتزويده بالبرامج اللازمة للاستفادة من هذه المساحة والتعامل معها، يدخل في مفهوم المال المنقول، حيث إن القرص الصلب، والبرنامج المثبت على الحاسب تعد أشياء مادية(١)، ذات قيمة مالية قابلة للانتقال من مكان لآخر دون أن تفقد

(١) وهذا ما استقرت عليه أحكام القضاء الفرنسي، حيث ذهبت في أحد أحكامها إلى توافر الشرط المسبق في جريمة خيانة الأمانة، والتي وقعت على المعلومات المسجلة على الفيش والأشرطة والملفات والخطط الصناعية، وذلك بالنظر إلى أن هذه الجريمة انما وقعت على الدعامات المادية، ولا توجد مشكلة قانونية في ذلك.

Crim,2/4/1974, crim, n 139, Juris-classeur periodique, ed. S,1974, n

خصائصها ومقوماتها، ومن ثم يتوافر فيها وصف المال المنقول وفقا للنص السابق[1].

ثانيا: أن يتم تسليم هذا المنقول بموجب عقد من عقود الأمانة. وهذا ما عبر النص السابق عنه ذلك صراحة. وعقود الأمانة هي الإيجار، والوديعة، والرهن، والوكالة، والعارية، حيث يجب أن يتم تسليم المال المنقول بموجب عقد من هذه العقود كشرط مسبق على وقوع جريمة خيانة الأمانة.

وقد تحقق هذا الشرط أيضا في العلاقة بين البنك الإلكتروني ومتعهد الإيواء. فالبنك يتسلم الأجهزة والبرامج المملوكة لمتعهد الإيواء لاستعمالها والانتفاع بها بموجب عقد الإيواء، الذي يعد وفقا للرأي الراجح عقد إيجار.

وبناء عليه توافرت الشروط المسبقة في جريمة خيانة الأمانة في علاقة البنك بمتعهد الإيواء. ومن ثم يتصور وقوع جريمة خيانة الأمانة من قبل البنك الإلكتروني في حالة قيامه بأي فعل يشكل ومن ثم اختلاسًا أو إساءة استعمال أو تبديدًا للأجهزة والبرامج المسلمة له من قبل متعهد الإيواء بموجب عقد الإيواء، وذلك كما لو سمح البنك لأحد المواقع بالاستفادة من الأجهزة المخصصة له من

186, Rec.D,1974,I.R, n 120:**Crim**,4/1/1968,Bull.crim,n 1, Rec. D, 1968, p496

مشار لهذه الاحكام لدى: **شيماء عبد الغنى محمد عطا الله**، مرجع سابق، ص ٧٩.

(١) بل لقد وصل بعض الفقه، إلى أبعد من ذلك، حيث أضفوا وصف المنقول على المعلومات الإلكترونية، وذهبوا إلى إعمال النص الخاص بجريمة السرقة على أي استيلاء يقع على هذه المعلومات. وسار على ذات الدرب العديد من أحكام القضاء، حيث ذهبت محكمة النقض الفرنسية إلى التخفيف من الطابع المادي للمنقول، وذلك من خلال النظر للأشياء المعنوية، كالمعلومات على انها منقولات مادامت لها قيمة مالية. المرجع السابق، ص ٤ وما بعدها.

قبل متعهد الإيواء بدون الحصول على إذن بذلك من متعهد الإيواء. أو أساء استعمال هذه الأجهزة والبرامج على نحو أدى إلى تلفها.

وعلى الرغم من قدرة القواعد العامة في قانون العقوبات على استيعاب إمكانية وقوع جريمة خيانة الأمانة من قبل البنك الإلكتروني، إلا أن هذا لا يمنع من ضرورة توجيه النداء إلى المشرع العقابي المصري، الذي يعلم جيدا حظر القياس في مسائل التجريم والعقاب بموجب نص الدستور، ويعلم أيضا الطبيعة الخاصة للمعاملات الإلكترونية على شبكة الإنترنت وما تحتاج إليه هذه المعاملات من معاملة خاصة تراعى طبيعة الأدوات المستخدمة في ارتكاب الجريمة، والبيئة التي تقع فيها. فمثلا أرى تحفظا على الإطار العام لنص المادة ٣٤١ سالفة الذكر، حيث تهيمن عليه الطبيعة المادية للمنقول محل الجريمة (مبالغ أو بضائع أو أمتعة أو تذاكر أو كتابات أخرى مشتملة على تمسك أو مخالصة) دون مراعاة للبيئة الافتراضية التي تتم فيها هذه المعاملات. هذا من ناحية.

من ناحية أخرى العبارات التي وردت في هذه المادة والخاصة بالأفعال التي تقع الجريمة من خلالها (اختلس أو استعمل أو بدد) لا تبدو كافية، حيث نتصور أن الجريمة يمكن أن تقع مثلا من خلال قيام البنك بعرض مواد غير مشروعة على موقعه المستضاف من قبل متعهد الإيواء دون علمه، أو إذنه في ذلك. لذلك يفضل وجود نصوص عقابية خاصة للانتهاكات التي تقع في البيئة الإلكترونية.

(ب) المسؤولية المدنية للبنك في مواجهة متعهد الايواء:

٩١- يسأل البنك الإلكتروني مدنيا في مواجهة متعهد الإيواء طبقا لما هو مقرر في خصوص مسؤوليته في مواجهة مقدم خدمة الدخول، ومصمم الموقع، لذلك

نحيل لما سبق ذكره[1]، وذلك منعا للتكرار.

---

(1) انظر سابقا، ص ١٥٠.

الفصل الثاني

الرقابة على البنك العامل عبر شبكة الإنترنت

٩٢- تضطلع الرقابة بدور كبير وفاعل في إنشاء وتشغيل البنوك بصورة عامة. وتستمد الرقابة دورها هذا، من طبيعة الأهداف المبتغاة من وجودها، والتي من أهمها تجنيب البنك والمتعاملين معه مخاطر العمل المصرفي بصورة عامة. فلاشك أن البنوك هي عصب الاقتصاد القومي في أي مجتمع، وذلك بالنظر إلى ما تضطلع به من خدمات وأنشطة ذات أهمية بالغة لكافة الأفراد داخل هذا المجتمع، خاصة التجار منهم، الأمر الذي يجب معه فرض معايير رقابية تسعى إلى التأكد من استيفاء البنك لكافة الضوابط والمعايير التي تؤهله لتقديم الخدمات المصرفية، والتأكد من استمرار توافر هذه المعايير بعد الإنشاء.

وتزداد أهمية الرقابة بهذا المعنى عند الحديث عن إنشاء وتشغيل البنوك على شبكة الإنترنت؛ وذلك بالنظر إلى الطبيعة الخاصة والجديدة للمخاطر التي تحيط بهذه البنوك، تلك المخاطر التي وجدت طريقها إلى هذه البنوك، تارة داخل البنك، نتيجة هيمنة التكنولوجيا ومفرداتها على العمل داخل البنك؛ حيث أفرزت مخاطر تتعلق بكيفية توظيف وتفعيل هذه التكنولوجيا في العمل المصرفي، ومخاطر أخرى تتعلق بافتقار الإدارات البنكية لمفهوم وطبيعة العمل المصرفي على شبكة الإنترنت، والذي لم يعد يصلح معه مجرد الفهم المحاسبي والقانوني فقط، بل يحتاج علاوة على ذلك، دراية وفهمًا للتكنولوجيا بأبعادها المختلفة، ليس على صعيد إدارة الأجهزة والبرامج فقط، ولكن أيضا على صعيد التعامل مع مقدمي الخدمات الإلكترونية اللازمة لتواجد البنك وتشغيله على شبكة الإنترنت.

وتارة أخرى خارج البنك، نتيجة تواصل البنك مع عملائه عبر شبكة الإنترنت، كوسيلة إلكترونية للاتصال عن بعد منفتحة على العالم بأسره، يغيب عنها وجود سلطة أو قوانين مركزية تحكم وتنظم تواجد وعمل البنوك عليها، مما ترتب عليه العديد من المخاطر الأمنية والقانونية. يضاف إلى كل ذلك البعد الدولي لنشاط هذه البنوك الذي أسفرت عنه شبكة الإنترنت، والذي أفرز مخاطر قانونية تستدعى الرقابة، نتيجة تقديم الخدمات المصرفية داخل دولة ما من قبل بنك يخضع لنظام قانوني في دولة أخرى.

ولما كانت هذه المخاطر حديثة العهد بالعمل المصرفي، فإن الأمر استدعى التعرف على طبيعة هذه المخاطر، وأهم صورها؛ وذلك من خلال التعرض لأهمية الرقابة ودورها في نظام عمل البنوك العاملة عبر شبكة الإنترنت، والتعرف على الوسائل الرقابية الكفيلة بمواجهة هذه المخاطر.

وبناء عليه، سوف نعرض في هذا الفصل لبيان أهمية الرقابة على البنوك العاملة عبر شبكة الإنترنت.(مبحث أول)، ثم للضوابط الرقابية التي تحكم إنشاء وعمل هذه البنوك (مبحث ثاني).

المبحث الأول

أهمية الرقابة على البنك العامل عبر شبكة الإنترنت

٩٣- يمس نشاط البنوك بصورة عامة مصالح عليا في الدولة، الأمر الذي يجعل خضوعها لرقابة صارمة أمرا مبررا. فالبنوك إجمالا هي المؤسسات القائمة على تداول النقود وصناعة الائتمان في أي دولة[١]، ومن ثم لا يمكن أن يطلق العنان لولوج هذا المجال دون وضع ضوابط معينة تحكم عمل وأداء هذه المؤسسات من ناحية، وتحمى المتعاملين معها من ناحية أخري، وذلك على النحو الذي يجعلها تعمل في تناغم مع إيقاع الاقتصاد القومي في مجموعه.

وقد كان لتدخل الدولة بإجراءات رقابية معينة على نشاط البنوك التقليدية أسباب تبرره، أهمها[٢]:

أولا: حماية الائتمان، الذي يعد وبحق عصب الاقتصاد الوطني، وركيزة التجارة الداخلية والخارجية، الأمر الذي فرض على الدولة ضرورة وضع الجهات القائمة على منحه وتوزيعه تحت سمعها وبصرها، وذلك حتى تضمن وتتأكد من قدرة وسلامة هذه المؤسسات على تحمل مسؤوليتها.

ثانيا: حماية المتعاملين مع البنوك. فالبنوك مؤسسات تقدم خدماتها لقاعدة عريضة من الأفراد (تجار وغير تجار)، الأمر الذي يبرر ظهور الرقابة

---

(١) د.حسين الماحى، مسؤولية البنك عن رفض منح أو تقديم الائتمان للمشروعات، مجلة البحوث القانونية والاقتصادية، كلية الحقوق ـ جامعة المنصورة، العدد (١٨)، أكتوبر ١٩٩٥، ص ١٢٧.

(٢) د.على جمال الدين عوض، مرجع سابق، ص٢٣.

على نشاط هذه البنوك حماية لهؤلاء الأفراد، ليس فقط من إنكار أموالهم، ولكن أيضا من ضياعها بسبب سوء إدارة هذه البنوك.

هذا وعلى الرغم من هذه الأسباب الهامة التي بررت تدخل الدولة للرقابة على إنشاء وعمل البنوك، إلا أن ذلك لم يجعل الدولة تغفل عن الطبيعة القانونية للبنك، وكونه في المقام الأول تاجرا يسعى وراء الربح وليس مرفقا عاما، الأمر الذي تطلب ضرورة ترك مساحة واسعة لحرية الحركة في إدارة ونظام عمل هذه البنوك[١].

وإذا كان ما سبق ذكره من أسباب توجب الرقابة على نشاط البنوك بصورة عامة (التقليدية والإلكترونية)[٢] لكن السؤال: هل تقديم الخدمات المصرفية من قبل بنك يعمل بصورة كاملة عبر شبكة الإنترنت كشف عن توجهات جديدة تستدعى تبنى مفهوم مختلف للرقابة على أعمال هذه البنوك؟

مما لا شك فيه أن ممارسة البنوك لنشاطها المصرفي من خلال شبكة إلكترونية للاتصال عن بعد كشبكة الإنترنت، تسبب في إحداث نقلة جذرية في صناعة الخدمات المصرفية، تلك النقلة التي ظهر أثرها في وجود بنك متكامل يعمل ويؤدى خدماته المصرفية على شبكة الإنترنت، مستغنيا بذلك عن الموجودات المادية (مباني ومعدات وأفراد)، مستبدلا بها مجموعة من الأجهزة الإلكترونية والبرامج المعلوماتية، مما انعكس كلية على مفهوم إنشاء البنك، وإدارته، وأسلوب تقديم الخدمة المصرفية والتواصل مع العملاء، كل هذا كان له

---

(١) المرجع السابق، ص٢٣.

(٢) د. طارق طه، إدارة البنوك في بيئة العولمة والانترنت، دار الجامعة الجديدة، ٢٠٠٧، ص ٤٦٨.

بالغ الأثر على أهمية الرقابة على عمل هذه البنوك، والتي يمكن لمس آثارها في ضوء الفوائد المتحصلة من وراء هذه النقلة، والمخاطر الناجمة عنها، وذلك على النحو التالي:

المطلب الأول

فوائد عمل البنك الإلكتروني على شبكة الإنترنت

٩٤- تتعدد الفوائد الناجمة عن عمل البنك على شبكة الإنترنت، ويأتي في مقدمة هذه الفوائد[(١)]:

١) السهولة والسرعة في تقديم الخدمات المصرفية. فتسخير وسيلة إلكترونية كشبكة الإنترنت في تقديم الخدمة المصرفية، من شأنه أن يسهل على البنك تقديم الخدمة المصرفية. فالبنك لم يعد يهمه اختيار الأماكن التي تنشط فيها حركة التجارة والصناعة كي يقيم له فرعا هناك، كما لم يعد في حاجة إلى مبأن ومعدات وأفراد لاستقبال العملاء وتلبية مطالبهم، بل أصبح الآن قادرًا على الإعلان عن خدماته المصرفية، والتعاقد عليها، وتنفيذها في أي دولة من دول العالم، بمجرد الضغط على مجموعة من المفاتيح الإلكترونية[(٢)]

(1)**Sofia Giannakoudi**,; Op. Cit, p. 207; **Jeanette Taft**, Op. Cit., p. 2.

(2) **Aleksander Berentsen**, Supervision and regulation of network banks, journal on the internet,2007, p1; **Richard J. Sullivan,** How Has the AdOption of Internet Banking Affected Performance and Risk in Banks?, Federal Reserve Bank of Kansas City _ financial industry perspectives 2000, p 1; **Yoonhee Tina Chang**, Dynamics of banking technology adOption: an application to internet bank-

ودون أن يكون حاصلا على ترخيص أو خاضعا للإشراف والرقابة من قبل هذه الدول[1]. أما عن العميل فلم يعد في حاجة إلى التعرف إلى عنوان البنك، والانتقال إلى مقره والانتظار في صفوف العملاء للحصول على الخدمة المصرفية، بل أصبح قادرًا على التعاقد على هذه الخدمة والحصول عليها دون أن يبرح مكانه، لمجرد أنه يمتلك جهاز كمبيوتر متصل بشبكة الإنترنت، ويعلم العنوان الإلكتروني للبنك على شبكة الإنترنت فيستطيع الحصول على ما يشاء من خدمات مصرفية.

٢) السعي الحثيث لتقديم أفضل الخدمات المصرفية لإرضاء العملاء[2]، حيث يسعى البنك العامل على شبكة الإنترنت إلى الوصول إلى أقصى مستوى في تقديم الخدمة المصرفية لجذب أكبر عدد من العملاء. ويعود هذا السعي لاحتدام المنافسة بين المؤسسات البنكية وغير البنكية في تقديم الخدمات المالية على شبكة الإنترنت لتقديم للوصول لأفضل مستوى من الخدمة وبأقل تكلفة[3]، الأمر الذي سيدفع بالبنوك إلى التسابق لإدخال تحسينات تكنولوجيا

---

ing, Warwick economic research paŗ ers- university of Warwick, No 664, January 2003, p. 3.

(1) **Nikos Bogonikolos,** DevelOpment of surveillance technology and risk of abuse of economic information, European Parliament, May 1999, (PE 168), p. 3; **Internet Banking**; Op. Cit, p. 5; **The new banking delivery system-the internet**, Goodwin, Procter& Hoar LLp, vol.2 No.35, April 27, 1999, p. 1; **Fethi Calisir-Cigdem Altin Gumussoy**; Op. Cit., p. 219.

(2) **Is auditing guideline internet banking**; Op. Cit, p. 2; **G C Chalikias,** Op. Cit, p. 3.

(3) Online banks heat up competition with savings rates of 5% or more, Academic Search Premier, FEB 13. 2007. available at:

متسارعة في مجالات الاتصالات، وأجهزة وبرامج الحاسب الآلي التي تعمل على معالجة المعاملات بسرعة وسهولة أكبر، وصولا لرضاء العميل[1]، ومن ثم تحقيق أقصى ربح ممكن[2].

٣) ظهور أشكال جديدة من الخدمات المصرفية، حيث تمكنت البنوك من استغلال معطيات التكنولوجية المعلوماتية في استحداث خدمات مصرفية جديدة، دعت إليها حاجة التجارة الإلكترونية على شبكة الإنترنت؛ مثل الدفع بالنقود الإلكترونية[3]، وخدمات الاطلاع على الحساب، والحصول على المعلومات المصرفية حول هذا الحساب[4]. وقد لعبت هذه الخدمات دورا كبيرا في إنجاح التجارة الإلكترونية عبر شبكة الإنترنت[5] .

---

http://www.bankrate.com/;**Electronic banking group initiatives and white Papers**, Basel committee for banking supervision, October 2000, p14. available at: www.bis.org/pub1/bcbs76.htm-17k.

(1) **Pormita shaha yanni zhao**, relationship between online service quality and customer satisfaction (a study in internet banking), Master thesis, department of businees administration and social sciences- lulea university, 2005, p 3

(٢) **د. سعيد الحامز**، مرجع سابق، ص٢٣٩٢.

(٣) **د. شريف محمد غنام**، محفظة النقود الإلكترونية، دار النهضة العربية، (بدون تاريخ نشر)، ص ٧.

(4) **Apostolos Ath. Gkoutzinis**, Op. Cit., p. 30.

(5) **Haibo Huang,** Essays in electronic money and banking, dissertation- faculty of the graduate school, university of Taxes, 2005, p. vii; See also: **Olga Lustsik**; Op, Cit, p. 5.

٤) انخفاض تكاليف العمل المصرفي[1]. فالبنك لم يعد في حاجة إلى مبان لاستقبال المتعاملين معه، ولا موظفين قائمين على استقبال هؤلاء المتعاملين وإدارة التعاقدات معهم. ولم يعد هؤلاء المتعاملين في حاجة إلى تكبد نفقات الانتقال والانتظار، حيث يستطيع البنك الإلكتروني التعامل مع عملائه عن طريق موقعه الإلكتروني على شبكة الإنترنت، دون حاجة إلى تكبد النفقات السابقة[2].

كل هذه الفوائد وأكثر نتجت عن عمل البنوك على شبكة الإنترنت، وجعلت من وجود هذه البنوك أمرا حيويا لا غنى عنه لأي دولة (متقدمة أو نامية) تسعى إلى الاستفادة من معطيات التجارة الإلكترونية على شبكة الإنترنت، الأمر الذي تتجلى معه أهمية الرقابة على إنشاء وعمل هذه البنوك؛ والذي يظهر من تأكد جهة الرقابة من استيفاء البنك لمجموعة من الضوابط والمعايير التي تؤهله للعمل بنجاح، ومن ثم تحقيق هذه الفوائد.

المطلب الثاني

مخاطر عمل البنك الإلكتروني عبر شبكة الإنترنت

---

(1) **G C chalikias,** Op. Cit, p. 2; **Adrian McCullagh and William Caelli** Op. Cit., p. 3; **James E Backhouse**, Security: The Achilles heel of electronic commerce, Computer security research center at the London school of economics, 1998. p. 30.

(2) **Electronic Banking Group Initiatives and White Papers**. Basel committee for banking supervision, Op. Cit, p. 16.

٩٥- وعلى الرغم من كل الفوائد السابقة، إلا أن هذا لم يمنع مَن وجود بعض التحفظات التي رافقت هذه الفوائد، وعكست في ذات الوقت بعض أشكال المخاطر، التي بررت وعظمت من أهمية الرقابة على البنوك الإلكترونية العاملة عبر شبكة الإنترنت(١).

وقد أكد هذا المعنى وأظهره التقرير الصادر عن البنك المركزي الهندى، الذي أوضح أهمية البنوك العاملة عبر شبكة الإنترنت، كما أظهر وجود أنواع جديدة من المخاطر الرقابية المرتبطة بأنشطة هذه البنوك(٢)، أهمها المخاطر الأمنية، والمخاطر القانونية، والمخاطر التشغيلية، وذلك على التفصيل التالي:

١)- المخاطر الأمنية (Security risks):

٩٦- تعد المخاطر الأمنية من أخطر وأهم القضايا التي تشغل فكر وبال كل من القائمين على إدارة البنوك العاملة عبر شبكة الإنترنت والمتعاملين معها(٣)، وذلك لسببين:

الأول/ الطبيعة الخاصة للنشاط المصرفي على شبكة الإنترنت، والذي تزداد فيه دواعي الأمن، وذلك بالنظر إلى الطبيعة المالية التي يقوم عليها النشاط المصرفي، والتي يزيد في ظلها الحرص على اعتبارات السرية والخصوصية،

---

(1) **Is auditing guideline internet banking**; Op. Cit., p. 3; **Gita Radhakrishna**, Op. Cit, p. 1

(2) this report available at: www.rbi.org.in/Scripts/PublicationReportDetails.aspx

(3) **Aleksander Berentsen,** Supervision and regulation of network banks, Op, Cit, p. 1; **Electronic Banking Group Initiatives and White Papers**, Op. Cit, p. 17.

انظر أيضا: يونس عرب، البنوك الإلكترونية، مرجع سابق، ص١٦.

والتي يرتبط صيانتها والحفاظ عليها بوجود البنك واستمرار نشاطه، باعتبارها تضرب بعمق في السمعة التجارية للبنك.

الثاني/ هيمنة الأجهزة والبرامج الإلكترونية على تشغيل البنك من قبل العاملين لدى البنك ومقدمي الخدمات الإلكترونية، والذي من شأنه أن يلوح بمخاطر أمنية مصدرها هؤلاء. أيضا البيئة الإلكترونية المفتوحة على العالم بأسره (شبكة الإنترنت) التي يحيا البنك ويؤدى خدماته في كنفها،على الرغم ما لها من فوائد يمكن أن يجنى البنك من ورائها مكاسب كبيرة، إلا أنها في ذات الوقت تكتظ بالمخاطر التي تهدد وجود البنك وتعاملاته مع العملاء[1]. هذه المخاطر من شأنها لو تمكنت من البنك لعصفت بوجوده، وأخذت بناصيته إلى الهاوية.

٩٧- وتجد مخاطر التهديد الأمني سبيلها إلى البنك الإلكتروني بناء على ذلك من اتجاهين:

الأول: التهديد الداخلي. ومصدره العاملين لدى البنك، الذين قد يشكلون مصدرا كبيرا للمخاطر الأمنية. فالعامل لدى البنك بحكم طبيعة عمله يستطيع الدخول على أجهزة البنك، والاطلاع على ما بها من بيانات، وإضافة وحذف ما يريد منها، الأمر الذي يلوح بمخاطر عظيمة، ويأخذ حكم العاملين لدى البنك في هذا الخصوص مقدمو الخدمات الإلكترونية (كمقدم خدمة الإيواء) الذين لهم اتصال دائم بالبنك لتشغيله فنيا على شبكة الإنترنت، والذين يملكون بموجب هذا الاتصال

(1)**Sofia Giannakoudi**;Op.Cit, p 208; **Zakaria I.Saleh**, An examination of the internet security and its impact on trust and adOption of online banking, Dissertation, Capella, 2003, p.11.

التعرض للبيانات الخاصة بالبنك[1].

الثاني: التهديد الخارجي. ومصدره كل المتعاملين مع شبكة الإنترنت من أصحاب النوايا الخبيثة (محترفين/هواة)، حيث تتعدد أشكال التهديدات التي يمكن أن يبارزوا بها البنك؛ مثل الدخول غير المشروع على الموقع الإلكتروني للبنك لسرقة البيانات الخاصة بتعاملات البنك مع عملائه[2]، أو تقليد موقع البنك على شبكة الإنترنت على النحو الذي يتسبب في خديعة المتعاملين معه، أو إرسال فيروسات لأجهزة البنك عبر شبكة الإنترنت، مما يكون سبب في تعطيل الأجهزة، وشل حركة التعاملات[3].

ويعد الشكل الثاني من أشكال التهديد من إفرازات شبكة الإنترنت، والتي تسمح لكل متصل بها أن يلج الموقع الإلكتروني للبنك، الأمر الذي لم يكن معروفا في ظل عمل البنوك التقليدية، حتى بعد استعانة هذه البنوك بأجهزة الحاسب في العمل المصرفي، أو حتى تكوين شبكة إلكترونية داخلية بالتعاون مع بعض البنوك لتسهيل بعض أشكال المعاملات المصرفية، فأن ذلك كله لم يكن يحمل ذات المخاطر التي تحملها شبكة الإنترنت كوسيلة اتصال إلكترونية مفتوحة على العالم بأسره، ولا يعتمد البنك عليها لمجرد الإعلان عن خدماته فقط، لكنه ينشأ ويمارس عمله على هذه الشبكة.

وعلى الرغم من هذا، إلا أن الدراسات أكدت أن نسبة التهديد الداخلي تفوق

---

(1) **Adrian McCullagh and William Caelli**, Op. Cit, p. 337; **Michael P. Dierks**; Op. Cit, p. 313; **Jean Pionnier**; Op. Cit, p. 155

(2) **David L. Baumer and others**; Op. Cit., p. 407.

(3) **Richard J. Sullivan**, Op. Cit, p. 3.

نسبة التهديد الخارجي بسبب امتلاك العاملين لدى البنك للمعرفة والخبرة الكافية للدخول على النظام والتعامل معه(١)، الأمر الذي ينذر بعواقب وخيمة أن لم يتحصن البنك بتدابير أمنية محكمة، ونظم رقابية فعالة تتأكد من توافر هذه التدابير، وتحسن التعامل معها بجدية(٢).

٩٨- وأيا ما كان اتجاه التهديد الأمني- والذي هو في حد ذاته خطر كبير- إلا أنه ينطوي على بعد أكبر من المخاطر، يتمثل في الاعتداء على سرية وخصوصية بيانات البنك الإلكتروني وعملائه، والتي من شأنها أن تفرض على البنك الإلكتروني تبنى نظم أمنية محكمة، على النحو الذي لا يسمح فيه بالمرور إلا للمخول له بذلك فقط(٣)، وذلك مع العلم أن هذه الأمور مرتبطة بسمعة البنك وموثوقيته(٤). ومن ثم لا بد من وجود إجراءات رقابية تضمن توافر هذه النظم وجدية تطبيقها(٥).

وهذا ما عظمت اللجنة الوطنية الأمريكية للتحويل الإلكتروني للأموال (US National Commission on Electronic Fund Transfers) من شأنه،

---

(1) **David L. Baumer and others,**; Op. Cit., p. 407.

(2) **Internet Banking**, comptrollers handbook, October 1999, p. 8.

(3) **Electronic Banking Group Initiatives and White Papers**, Basel committee for banking supervision, Op. Cit., p. 17.

(٤) **د. سعيد الحامز**، المرجع السابق، ٢٣٩٢.

Jeanette Taft; Op, Cit, p. 44

(5) **Nikos Bogonikolos**; Op. Cit, p.3; **Jon M. PEHA**, Electronic commerce with verifiable Audit Trails, available at: http://www.chicagofed.org/consumer_information/what_you_should_know_about_internet_banking.cfm

- **John Skip Benamati - Mark A. Serva**; Op. Cit, p172.

حيث ذهبت إلى أن البنك الإلكتروني العامل عبر شبكة الإنترنت يقوم نشاطه في مجموعه على تدفق المعلومات، والبيانات سواء داخل الشبكة الداخلية للبنــك، أو عبر شبكة الإنترنت، الأمر الذي تدق معه أجراس الخطر لحماية سرية وسلامة هذه المعلومات من الاطلاع غير المشروع عليها أو المساس بسلامتها(١).

٩٩- ويبدو لنا أنه يضاف إلى كل ما سبق ذكره من مخاطر تأكيدا على أهميــة الرقابة من الناحية الأمنية على البنوك الإلكترونية العاملة عبر شبكة الإنترنــت أمران:

الأول: وجود فراغ تشريعي على الصعيدين الجنائي والمدني ــ خاصة في العديد من الدول النامية ــ لمواجهة الاعتداءات الأمنية على شبكة الإنترنــت؛ والــذي يبرر بعالمية الشبكة وصعوبة وجود قوانين مركزية لمواجهة هذه الاعتداءات(٢)، الأمر الذي لا يبقى معه للبنك والمتعاملين معه من ضـــمانات لمواجهـــة هــذه المخاطر سوى الرقابة؛ والتي ستظهر في صورة ضوابط أمنية تفرضـــها جهـــة الرقابة على البنك وتلزمه بها حتى يرخص له بالإنشاء وممارسة نشاطه، هــذه الضوابط التي تراعى فيها جهة الرقابة التأكد من استعدادات البنك الأمنية علـــى الصعيدين الداخلي والخارجي؛ من خلال استعمال الأجهزة والبرامج الأمنية التي تعمل على التصدي للمخاطر، أيضا من خلال فرض البنك نـــوع مـــن الرقابـــة الداخلية علة نشاط العاملين لديه ونشاط مقدمي الخدمات الإلكترونية. كل ذلك من شأنه أن يؤكد أهمية الرقابة على المخاطر الأمنية، ويجعلها بمثابة حصن يحتمي

---

(1) **Apostolos Ath. Gkoutzinis**;Op. Cit, p. 149; **Everett Durante Cordy**; Op. Cit, p. 403

(2) **Nicholas Imparato,** public policy and the internet, Hoover Institution Press, p. 15.

بها البنك والمتعاملين معه في ظل غياب الضمانات التشريعية.

الثاني: أن قضية التهديد الأمني في حياة البنك العامل عبر شبكة الإنترنت لا تبدو أهميتها في مرحلة إنشاء البنك على هذه الشبكة فقط، ولكنها تظل مخيمة بظلالها طوال فترة عمل البنك، الأمر الذي تبدو معه أهمية الإشارة إلى ضرورة تناسب الضوابط الأمنية مع حجم تعاملات البنك من ناحية، وديمومة عملية الرقابة على إعمال هذه الضوابط من ناحية أخري.

وبناءً عليه يمكن القول بأن المخاطر الأمنية أيا ما كان اتجاهها، وأيا ما كانت طبيعة الشخص الذي يقف وراءها فإنها بلا شك ذات انعكاسات خطيرة على وجود البنك ونشاطاته، وتنذر بعواقب لا حصر لها، أهمها فتح باب المسؤولية القانونية للبنك على مصراعيه في مواجهة عملائه، باعتباره المسؤول الأول عن تأمين المعاملات المصرفية تجاه عملائه، والأمر على هذا النحو من شأنه أن يهدد استمرار تشغيل البنك، وذلك كله ما لم يتحصن البنك بحصون أمنية صلبة ومحكمة، تحت سمع وبصر جهة رقابة تتأكد دائما من وجود وفاعلية هذه الحصون، خاصة في ظل النظام الذي يقوم عليه تأمين أية مؤسسة تعمل على شبكة الإنترنت؛ وهى أن كل منظمة مسئولة عن تأمين وجودها ومعاملاتها بصورة ذاتية؛ نظرا لغياب سلطة مركزية تعمل على فرض قواعد أمنية موحدة، وفى ظل غياب التنسيق بين المنظمات المختلفة العاملة على شبكة الإنترنت[١].

---

(1) **Aaron J. Burstein**, Amending the ECPA to enable a culture of cybersecurity research, Harvard journal of law & Technology Vol. 22, Number 1 , 2008, p 171

٢)- المخاطر القانونية (Legal Risks):

١٠٠- تعد المخاطر القانونية من أهم صور المخاطر التي تؤرق كل المتعاملين بالتجارة الإلكترونية بوجه عام والبنوك العاملة عبر شبكة الإنترنت بوجه خاص(١). ومبعث هذا الأرق يكمن في التكنولوجيا ومفرداتها، والذي تجلى في اتجاهين مترابطين:

الأول/ تسببت هذه التكنولوجيا في إحداث طفرة كبيرة في أسلوب تقديم الخدمات المصرفية، انعكست بدورها على طبيعة التنظيم القانوني الخاص بهذه الخدمات، حيث باتت معظم القواعد المصرفية التقليدية غير قادرة على استيعاب هذه المستجدات.

الثاني/ أن هذه التكنولوجيا تتسم بالتطور المستمر والمتلاحق، الذي قد لا يستطيع المشرع أن يلحق بركابه، على النحو الذي يتسبب في وجود حالة من الفراغ التشريعي، والذي يتجلى في صورة عدم قدرة القوانين القائمة على ملاحقة هذه التطورات، واستيعاب الفروض المختلفة لها.

كل من هذين الاتجاهين يؤديأن في النهاية إلى مخاطر قانونية نتيجة عدم وجود نصوص ترعى وتحمى المتعاملين مع هذه البنوك، بما يشكل تهديدا لحقوق هؤلاء المتعاملين(٢). وقد أكدت المحاكم الأمريكية أنه على الرغم من توافر

---

(1) **Electronic Money**, Report of the working party on electronic money (Group of ten), April 1997, p 4. Available at: http://www.bis.org

(2) **Anita K. Pennathur**, Clicks and brick: e-risk management for banks in the age of the internet, journal Of banking & finance, 2001, p. 2112.

العديد من تطبيقات التكنولوجيا الأمنية في مجال المعاملات الإلكترونية، إلا أنها مع ذلك تقف عاجزة عن تحقيق الأمن الكافي، الأمر الذي تبدو معه وتتجلى أهمية التشريعات الصارمة التي توفر غطاء كافيا وكفيلا بتحقيق الحماية اللازمة(١).

١٠١- وتعرف المخاطر القانونية في حياة البنوك العاملة عبر شبكة الإنترنت بأنها عبارة عن "حالة من عدم التوافق بين التشريعات والعادات المستقرة والمعايير الأخلاقية، وبين نظام عمل البنك، وذلك على النحو الذي يجعل تعاملات البنك مع عملائه يشوبها الغموض وعدم الاستقرار"(٢).

١٠٢- وتتعدد صور المخاطر القانونية الناتجة عن التزاوج الذي تم بين العمل المصرفي ونظم التكنولوجية الحديثة، والتي من أهمها:

١) مخاطر انتهاك السرية(٣)، والتي يرتبط الحفاظ عليها بوجود البنك من عدمه، حيث تتوهج خطورتها من الترابط غير المتناهي بين المواقع الإلكترونية على

انظر أيضا: **يونس عرب**، البنوك الإلكترونية، المرجع السابق، ص ١٤.

Richard J. Sullivan; Op. Cit. p. 12; **Jennifer Iser**; Op. Cit. p. 53.

(1) **David L. Baumer and others**; Op. Cit., p. 407; **Roger Dean and others,** Identity management – back to the user, December 2006, Network Security, p 6.

(2) **Internet Banking;** Op.Cit,p.9.

(3) **Electronic banking group initiatives and white Papers**; Op. Cit., p. 20; **William Gram**; Op. Cit., p18 ; **Jon M. Peha- Ildar Khamitov**. Pay Cash: A secure efficient internet payment system, International conference on electronic commerce, 2003. p. 9. **Bank of Internet USA,** Privacy policy. january 2006, available at: http://www.bankofinternet.com/privacy-policy.aspx

شبكة الإنترنت. ومخاطر السرية ليست صاحبة بعد أمنى يحتاج إلى الاستعانة بأجهزة وبرامج أمنية قوية وحسب، بل هي صاحبة بعد قانوني ذات تأثيرًا أعمق، حيث إن غياب تشريعات تلزم البنك والعاملين لديه ومقدمي الخدمات الإلكترونية بالحفاظ على سرية البيانات الخاصة بالعملاء أمر يشكل خطورة فادحة، حتى في ظل استعمال البنك لأقوى النظم الأمنية، الأمر الذي يمكن أن يتم التخفيف من غلوائه بإلزام البنك بفرض الحفاظ على سرية البيانات المصرفية على العاملين لديه ومقدمي الخدمات الإلكترونية في عقود تشغيلهم، وذلك تحت رقابة صارمة من قبل جهة الرقابة، التي تعمل على التأكد من توافر هذه الضوابط والمعايير على نحو يحقق أقصى حماية ضد مخاطر انتهاك السرية.

٢) مخاطر غسيل الأموال وقواعد المسؤولية بخصوصها، خاصة أن البنوك العاملة عبر شبكة الإنترنت تعد عاملا مساعدا قويا لارتكاب مثل هذه الجرائم بالنظر لما تتميز به من سرعة كبيرة في إجراء المعاملات المصرفية، وعدم التقيد بالحدود الجغرافية عند إجراء هذه المعاملات(١)، الأمر الذي يعظم من دور الرقابة على مدى التزام البنوك بمراعاة الضوابط الخاصة بمكافحة جرائم غسل الأموال عند تعاملها مع عملائها.

---

(1) **Turnerr Shawn,** U.S. anti-money laundering regulation: an economic approach to cyber laundering, case western reserve university school of law, Vol. 54:4, 2004, p 1407; **Jennifer Iser**; Op. Cit, p. 49; **Money Laundering**; Op. Cit p. 15; Gita Radhakrishna, Op. Cit, p. 1

انظر أيضا د. **صفوت عبد السلام عبد الله**، الآثار الاقتصادية لعمليات غسيل الأموال ودور البنوك في مكافحتها، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، غرفة تجارة وصناعة دبي، ٩-١١ ربيع الأول هـ ١٤٢٤/١٠-١٢ مايو ٢٠٠٣م، ص١٥٤٧.

٣) مخاطر حماية المستهلك، الأمر الذي يشكل خطورة كبرى على عملاء البنك، نتيجة إخضاعهم لشروط تعسفية من قبل البنك، الأمر الذي يؤكد دور الرقابة، للتأكد من اتباع البنك لقواعد حماية المستهلك في معاملات البنك مع العملاء.

كل هذه الصور وغيرها كانت مبعثا للمخاطر، وأظهرت الحاجة الماسة للرقابة على عمل هذه البنوك للتأكد من مراعاتها لحقوق المتعاملين معها والحفاظ عليها.

والسؤال: إلى أي مدى يمكن أن تؤثر المخاطر القانونية بالمعنى السابق على البنك وعملائه؟

١٠٣- يمكن الإجابة على هذا التساؤل بالقول بأن المخاطر القانونية وتبعاتها المختلفة بالمفهوم السابق ذات تأثيرًا كبير على عملاء البنك الإلكتروني والبنك نفسه، وذلك على النحو التالي:

- فبالنسبة لعملاء البنك الإلكتروني، فإنهم يتضررون كثيرا نتيجة عدم التزام البنك بالضوابط القانونية التي تحكم عرضه لخدماته المصرفية، وكيفية الإعلان عنها عبر الموقع الإلكتروني للبنك، وتزويدهم بالمعلومات والبيانات الكافية حول طبيعة هذه الخدمات، وكيفية التعاقد بشأنها[1]. كذلك عدم مراعاته لوضع علامته التجارية، ورقم قيده في السجل التجاري. أيضا عدم اكتراث البنك بأصول التعاقد النموذجي عبر شبكة الإنترنت في نماذج العقود المصرفية التي تحكم تقديمه لخدماته[2]. يضاف إلى ذلك، أنه في ظل غياب تنظيم قانوني يحكم تعاقدات البنك

---

(1) **Comptroller of the Currency**. Administrator of national banks, corporate decision# 99-50, January 2000, p. 1.

(2) **Richard J. Sullivan**; Op. Cit, p. 12.

مع عملائه، قد لا يلزم البنك نفسه في تعاقداته مع العملاء بالحفاظ على سرية بياناتهم، أو يلزم نفسه ولكن لا يشدد من أحكام مسؤوليته بخصوصها، بما لا يتلاءم مع طبيعة التعاملات المصرفية عبر شبكة الإنترنت، وذلك على النحو الذي يشكل خطراً كبيرا على حقوق هؤلاء العملاء. أيضا يمكن أن يشكل غياب التنظيم القانوني خطرا على العملاء من حيث قيام البنك بفرض جزاءات مالية أو عقدية (كفسخ العقد) على العملاء على نحو مبالغ فيه، الأمر الذي يشكل خطرا على هؤلاء العملاء.

- أما بالنسبة للبنك الإلكتروني فغياب تنظيم قانوني فعال يحكم ويوجه تعاملاته على النحو الموضح بخصوص العملاء من شأنه أن يفضي في النهاية إلى فقدان البنك لسمعته بين المتعاملين معه[1]، والتي تعد بحق رأس المال الحقيقي للبنك، الأمر الذي يشكل بداية النهاية لهذا البنك.

ومن هنا تسطع وتتجلى أهمية الرقابة على عمل البنوك الإلكترونية العاملة عبر شبكة الإنترنت، والتي هي بمثابة ضمانة وحصانة لكل من البنك وعملائه، حيث تعمل جهة الرقابة على التأكد بصورة مستمرة من مراعاة البنك والتزامه بالضوابط الرقابية التي توجه البنك دائما إلى الالتزام بالقوانين السارية، والتأكد من عدم الإجحاف بحقوق العملاء في حالة غياب هذه القوانين، وذلك في كافة نشاطات البنك بداية من إنشائه، مرورا بإعلانه عن خدماته وتعاقداته مع عملائه، وانتهاءً بحصول هذا العميل على الخدمة[2].

---

(١) د. سعيد الحامز، المرجع السابق، ص٢٣٩٢.

(2) **Internet Banking**; Op. Cit. p. 9; **Richard J. Sullivan**; Op. Cit, p. 12.

١٠٤- وتأخذ المخاطر القانونية في حياة البنك الإلكتروني العامل عبر شبكة الإنترنت بعدا جديدا، تسببت فيه الطبيعة الدولية للنشاط المصرفي للبنك على شبكة الإنترنت(١). فشبكة الإنترنت كوسيلة عالمية للاتصال عن بعد مكنت البنك من مخاطبة العالم بأسره بخدماته، الأمر الذي أضفى على نشاطه طابعا دوليا، على الرغم مما جلبه على البنك من فوائد، إلى أنه حمل بين طياته بعض المخاطر القانونية، والتي تمثلت أهمها في:

أ- القدرة المطلقة للبنك العامل عبر شبكة الإنترنت على عبور الحدود الوطنية، والجمع بين أنشطة مصرفية تخضع بطبيعتها للإشراف والرقابة (باعتبارها تمثل الحد الأدنى المتعارف عليه من الأنشطة المصرفية التي تجمع جهات الرقابة على خضوعها للرقابة)، وأنشطة قد لا تكون خاضعة للرقابة من قبل دولة البنك، ولكنها تخضع للرقابة من قبل سلطات الرقابة في الدولة التي يتعاقد أحد المقيمين فيها مع البنك بخصوص أحد خدماته، الأمر الذي يشكل انتهاكا لقوانين الرقابة في هذه الدولة، حيث يؤدى البنك فيها خدمات مصرفية لم يخضع بخصوصها للإجراءات الرقابية المطلوبة، الأمر الذى يمثل خطورة على دولة المتعاقد مع البنك (٢).

ب- الصعوبات العملية التي يمكن أن تواجه السلطات الوطنية، والتي ترغب في التعامل إداريا أو قضائيا مع مواقع بنوك إلكترونية تعمل في مناطق سيادية

(1) **Jennifer Iser**; Op. Cit, p. 53; **Report on electronic money**, European central bank; Op. Cit, p. 6.
(2) **Apostolos Ath. Gkoutzinis**, Op. Cit, p. 19.

أخرى، لا يوجد بينها وبين السلطات الوطنية تعاون[١].

ج- المشاكل الناجمة عن تنازع الاختصاص القانوني والقضائي عند وقوع منازعات بسبب أحد العقود المصرفية التي أقامها البنك مع أحد عملائه المقيم في دولة غير دولة البنك، مما يشكل مخاطر تتعلق بتحديد المحكمة المختصة بنظر النزاع والقانون الواجب التطبيق، مما يؤدى إلى احتمالية ضياع الحقوق، أو حتى تأخير الحصول عليها[٢].

ولاشك في خطورة المشاكل الدولية الناجمة عن دولية نشاط البنك على شبكة الإنترنت بالمعنى السابق، بل لعلها أحد أهم الصعوبات التي لا تواجه جهات الإشراف والرقابة، بل تواجه البنوك والمتعاملين معها، والتي أخذت بعض البنوك العاملة عبر شبكة الإنترنت في محاولة الحد من هذه الآثار والمشاكل عن طريق قصر التعاقد على خدماتها المصرفية على الدولة التي تخضع لقوانينها، أو في إقليم معين محيط بها[٣]. ولاشك أن في هذا الحل ما يفوت على البنك فرص الاستفادة من دولية شبكة الإنترنت، وما قد يعود عليه من وراء ذلك من مكاسب كبيرة الأمر الذي لا يشكل من وجهة نظرنا سوى تسكين مؤقت لهذا المرض العضال، الذي لا أرى حلا له سوى وجود نوع من التعاون الدولي الذي يسفر عن اتفاقيات دولية تضع آلية للتعاون بين جهات الإشراف والرقابة لتغطية

---

(١) **د. سعيد الحاسر**، مرجع سابق، ص٢٣٩٣.

(2) **Apostolos Ath. Gkoutzinis**,Op. Cit, p. 19.

(٣) **د. أسامة أبو الحسن**، المرجع السابق، ص ٧٦؛ انظر أيضا **د. فايز عبد الله الكندرى**، التعاقد عبر شبكة الانترنت في القانون الكويتي، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص ٦٠٥.

ومواجهة هذه المشاكل.

كل هذه الصور والأبعاد الخاصة بالمخاطر القانونية المحيطة بعمل البنك الإلكتروني عبر شبكة الإنترنت من شأنها أن تفرض وبقوة الحاجة الماسة والملحة لمجموعة من الضوابط الرقابية التي تفرض على البنك، والتي يقف من ورائها ويسهر على تطبيقها جهة رقابية حصيفة، تعتنق معايير رشيدة ومنضبطة، تسعى من ورائها لفرض سياج قانوني يحمي الاقتصاد القومي في مجموعه من خلال إخضاع ممارسة البنك لنشاطه على شبكة الإنترنت للقانون.

٣)- المخاطر التشغيلية(Operational Risks):

١٠٥- تعد المخاطر التشغيلية في نظام عمل البنوك من أهم صور المخاطر التي تسترعى اهتمام جهات الرقابة. ويعود ذلك إلى طبيعة المؤسسة محل الرقابة، من حيث كونها مؤسسة قائمة على تسيير حركة النقود في الدولة، ومسئولة عن تنشيط الائتمان فيها، وارتباط هذه الأمور بصورة مباشرة بطريقة تشغيل البنك، وإدارته(١)، وإذا كان هذا الحديث يشمل كلا من البنوك التقليدية والإلكترونية، فإن الأخيرة بلا شك تضيف إلى الاعتبارات السابقة اعتبارات أخرى تتعلق بمخاطر إدارة وتشغيل البنك في البيئة الإلكترونية.

١٠٦- وقد عرفت المخاطر التشغيلية في نظام عمل البنوك العاملة عبر شبكة الإنترنت من قبل تقرير لجنة بازل للبنوك الإلكترونية(٢) بأنها عبارة عن

---

(1) **Anita K. Pennathur**; Op. Cit., p. 2112; **Apostolos Ath. Gkoutzinis**;Op. Cit., p. 148

(٢) ولجنة بازل للبنوك الإلكترونية عبارة عن منتدى دولي للتعاون في مجال الإشراف والرقابة على البنوك، يعمل على تعزيز فهم القضايا الرقابية ومستجداتها، خاصة في

(احتمالية الخسارةِ بسبب ضعف كبير في الثقةِ وسلامةِ النظام)[1].

ويلاحظ على هذا التعريف عدم الدقة، بالإضافة إلى أنه حصر الأسباب المؤدية لهذه المخاطر في سببين فقط؛ ضعف كبير في الثقةِ، وسلامةِ النظام.

وبناء عليه يمكن لنا أن نعرف هذه المخاطر بأنها عبارة عن التهديدات الناتجة عن سوء إدارة البنك الإلكتروني وتشغيله على شبكة الإنترنت.

١٠٧- وقد تحلى هذا النوع من المخاطر بثوب الخصوصية في نظام عمل البنك الإلكتروني العامل عبر شبكة الإنترنت، وذلك للأسباب التالية:

أ- المخاطر الناجمة عن عمل النظم التكنولوجية في حالة إساءة اختيارها، أو إساءة تشغيلها من قبل القائمين على تشغيل البنك[2]؛ وذلك بالنظر إلى الاعتماد الكبير على الأجهزة إلكترونية والبرامج المعلوماتية الموثوق بها

مجال العمل المصرفي الإلكتروني، والعمل على رفع مستوى سلطات الرقابة حول دول العالم. وتعمل هذه اللجنة في سبيل تحقيق هذه الأهداف على تبادل المعلومات والبيانات بين السلطات الرقابية، ومحاولة تقريب وجهات النظر فيما يتعلق بالمخاطر الناجمة عن استعمال الوسائل الإلكترونية في البنوك، وذلك بهدف التوصل إلى معايير موحدة تحكم التصدي للمشاكل الرقابية، خاصة ما تعلق منها بالمشاكل الدولية. وتضم هذه اللجنة في عضويتها دول بلجيكا وكندا وفرنسا وألمانيا وإيطاليا واليابان ولوكسمبورج، وهولندا، وأسبانيا والسويد وسويسرا والمملكة المتحدة وأمريكا، حيث يتم تمثيل كل دولة من قبل بنكها المركزي. /http://www.bis.org/bcbs

Jeanette Taft; Op. Cit., p. 35.

(1) **Risk management principles for electronic banking**, Basel committee publication, July 2003, p. 1. Available at: http://www.bis.org/pub1/bcbs98.htm

(2) **Jennifer Iser**; Op. Cit., p 47; **John Skip Benamati - Mark A. Serva**; Op. Cit, p. 170.

(لتكفل أمن وسلامة المعلومات) لتشغيل وإدارة البنك، داخليا بين وحدات البنك الإلكتروني المختلفة، وخارجيا بين البنك وبين المؤسسات الأخرى[١]، الأمر الذي تظهر معه الحاجة للرقابة على كيفية اختيار هذه الأجهزة والبرامج من قبل إدارة البنك. ليس هذا فحسب بل إن اضطلاع الأجهزة الإلكترونية بالدور الأكبر في تسيير مجريات العمل المصرفي ينذر بعدم قدرة هذه الأدوات في بعض الظروف الخاصة على استيعاب الحجم الهائل للصفقات والمعاملات المصرفية (أوقات ضغط العمل)، أو وقوع أي حادث فجائي آخر، الأمر الذي يجب معه التأكد من استعداد البنك لمواجهة مثل هذه الظروف الطارئة (Contingency circumstance)، وذلك من خلال تبنيه لخطط تشغيل بديلة تشتمل على بدائل سريعة وفعالة لضمان سير العمل المصرفي بانتظام. وقدرة إدارة البنك على تنفيذ خطة الطوارئ[٢].

ب- وجود إدارات بنكية وموظفين يفتقرون في الغالب للخبرة اللازمة في التعامل مع الأجهزة الإلكترونية والبرامج، ومخاطر استخدامها في العمليات المصرفية الإلكترونية[٣]. فتشغيل البنك الإلكتروني على شبكة الإنترنت لا يكتفي بمصرفيين أصحاب خبرة في العمل المحاسبي فقط، ولكن أيضا في عمل الأجهزة الإلكترونية والشبكات[٤]، الأمر الذي سيفرض الحاجة إلى

---

(1) **M.Sklira. A.S.pomportsis. M.S. Obaidat**;Op. Cit,p1776;**Michael P. Dierks**; Op. Cit, p. 314

(2) **Internet Banking**; Op. Cit, p. 8.

(٣) **د. سعيد الحامز**، مرجع سابق، ص٢٣٩٢؛ انظر أيضا: **يونس عرب**، المرجع سابق، ص١٢.

Jeanette Taft; Op. Cit., p. 35.

(٤) **هشام صلاح الدين زكي**. تأثير التجارة الإلكترونية على البنوك،، أكاديمية السادات

نموذج جديد للعامل لدى البنك الإلكتروني، وذلك على النحو الذي يمكن معه القول إن إساءة اختيار العاملين لدى البنك أو التقصير في تدريبهم من كافة النواحي، أمر يهدد بمخاطر جمة، ويفرض الحاجة إلى وجود نظم رقابية فعالة للتأكد من تأهيل هؤلاء العاملين على النحو الذي يمكنهم من القيام بالأعمال المنوطة بهم.

جـ - الاعتماد الكبير على مقدمي الخدمات الإلكترونية لتشغيل البنك على شبكة الإنترنت[١]. فلا شك في الدور المحوري الذي يضطلع عليه هؤلاء في وجود وتشغيل البنك على شبكة الإنترنت، الأمر الذي قد يلوح بمخاطر لا حدود لها، مصدرها هؤلاء، وذلك على النحو الذي تظهر معه وتتجلى أهمية الرقابة على اختيار البنك لمقدمي الخدمات الإلكترونية العاملين لديه، وذلك من خلال التأكد من تأهيلهم الفني المناسب، وحصولهم على التراخيص التي تسمح لهم بممارسة عملهم، ومدى التزامهم بواجبات السرية والخصوصية[٢].

كل هذه المظاهر الخطرة مجتمعة تصب في النهاية في بوتقة واحدة، وتنذر بعاقبة مؤكدة، وهي عدم القدرة على تشغيل البنك الإلكتروني[٣]، أو بمعنى أخر عدم القدرة على تنفيذ التعاقدات المصرفية التي تحكم تقديم البنك لخدماته عبر شبكة الإنترنت، بما يؤدى حتما إلى قيام مسؤوليته عن هذا الإخلال، بما يستتبع فقدان البنك لثقة عملائه فيه، الأمر الذي قد يؤدى إلى توقف البنك عن العمل

للعلوم الإدارية- سلسلة إصدارات البحوث الإدارية (٣)، ٢٠٠١، ص ٦٧.

(١) يونس عرب، البنوك الإلكترونية، مرجع سابق، ص١٨.

(2) **Risk management principles for electronic banking,** Basel Committee Publication; Op. Cit, p. 1.

(3) **Internet Banking**; Op. Cit, p. 8.

بسبب ذلك.

كل هذه الأسباب كانت منبعا متدفقا للمخاطر على النحو الذي يفرض على إدارة البنك الإلكتروني ضرورة وضع خطط إستراتيجية منظمة، وسياسات محكمة، وإجراءات غاية في الدقة على نطاق المؤسسة البنكية بأكملها تراعى تنظيم عمل الأجزاء المختلفة الداخلة في تكوين البنك بشكل متجانس ومتناغم، وذلك على النحو الذي من شأنه أن يقلص إلى أقصى درجة حدة المخاطر التي يمكن أن تحدث.

١٠٨- وإدراكا من البنك المركزي المصري لأهمية البنوك العاملة عبر شبكة الإنترنت، وحرصا من جانبه على توفير مناخ رقابي فعال لهذه البنوك؛ فقد أصدر مجموعة من الضوابط الرقابية، التي أعتمدها مجلس إدارة البنك المركزي المصري في جلسته المنعقدة بتاريخ ٢٨ فبراير ٢٠٠٢ لإلزام البنوك الإلكترونية المسجلة لديه بها. وقد جاء فيها ذكر للأسباب التي تستلزم حصول البنوك على ترخيص لتقديم العمليات المصرفية الإلكترونية وهى[١]:

١)- حماية السوق المصرفي المحلى من مقدمي الخدمات المصرفية غير المرخص لهم من البنك المركزي المصري بتقديم هذه الخدمات، بما في ذلك الجهات التي ترغب في تأسيس كيان مستقل لا يتواجد له فروع مادية بغرض تقديم العمليات المصرفية الإلكترونية فقط virtual bank.

---

(١) **الضوابط الرقابية للعمليات المصرفية الإلكترونية وإصدار وسائل دفع للنقود الإلكترونية**، البنك المركزي المصري، الجلسة المنعقدة بتاريخ ٢٨ فبراير ٢٠٠٢. ص٢، انظر العنوان التالي:

http://www.cbe.org.eg/public/Regulations%20of%20The%20Electronic%20Banking%20Operations.doc

٢)- التحقق من توافر الوسائل الكافية لدى البنوك للإدارة الحصيفة لمخاطر تلك العمليات.

٣)- تطبيق الضوابط الرقابية اللازمة لحصول البنوك على ترخيص من البنك المركزي المصري لتقديم تلك العمليات.

١٠٩- أيضا أوصى تقرير لجنة بازل للبنوك الإلكترونية(١) بوجوب تبنى إدارات البنوك العاملة عبر شبكة الإنترنت لنظم إدارية جديدة، على أن تشتملِ هذه النظم على أدوات تمكنها من مواجهة المخاطر المرتبطة بنظم التكنولوجيا، وبالأفراد القائمين على تسيير هذه التكنولوجيا. كما أوصى التقرير ذاته الجهات الرقابية بضرورة مراعاة الطبيعة الجديدة لنظام إدارة العمل المصرفي، وذلك من خلال فرض إجراءات رقابية صارمة وشاملة لمواجهة كافة المخاطر المصاحبة للعمل المصرفي على شبكة الإنترنت، وفي ذات الوقت مراعاة ترك مساحة للبنك للابداع والتطوير في ممارسة العمل المصرفي من خلال حسن تفعيل التكنولوجيا وتسيير العمل المصرفي من خلالها، ومراعاة إجراء تطورات بصورة مستمرة.

١١٠- أيضا أوصى مكتب الرقابة على النقد الأمريكيOCC (Office of the Comptroller of the Currency)(٢) بضرورة تيقظ البنك عند قيامه باختيار الموظفين لديه بوضع قواعد صارمة ودقيقة في اختيار هؤلاء الموظفين، حيث يراعى فيها اختبار قدراتهم على التعامل مع نظم الحاسب والشبكات. كما يجب

---

(1) **Risk Management principles for electronic banking,** basel committee publication; Op. Cit., p. 2.

(2) **Decision of the Office of the Comptroller of the Currency on the application to charter,** Conditional Approval (347), January 2000,p. 4 - 5.

أن يقوم بهذه الاختبارات بصورة دورية. يضاف إلى ذلك وجوب قيام البنك بتدريبهم على كل ما هو جديد في خصوص الأجهزة التي تعمل على شبكة البنك[١]، كما يجب أن يحرص البنك على إلزام من يقومون بتوريد الأجهزة والبرامج له، بضرورة تزويد العاملين لدى البنك بكافة المعلومات التي تحيط بعمل هذه الأجهزة والبرامج، وذلك على النحو الذي يجعلهم قادرين على التعامل معها بسهولة ويسر (الالتزام بالإعلام)[٢].

١١١- وإذا كان الحديث السابق قد تفرغ لعرض صور المخاطر التي يمكن أن يتعرض لها البنك الإلكتروني بمناسبة تقديمه لخدماته عبر شبكة الإنترنت، بما استتبع ذلك من الإشارة إلى أهمية التزام البنك الإلكتروني بمراعاة هذه المتغيرات بما يتواءم مع طبيعة هذه المخاطر، فإن هذا الحديث لا يكتمل معناه دون الإشارة أيضا إلى أهمية التزام جهات الرقابة بمراعاة هذه المتغيرات عند صياغة الضوابط الرقابية التي تحكم عمل هذه البنوك، وذلك على النحو الذي يدفع هذه الجهات إلى ضرورة تبنى سياسات إشرافية جديدة تتلاءم مع الطبيعة الجديدة للعمل المصرفي، بحيث تحرص كل الحرص على فرض قواعد رقابية صارمة، وفعالة تضمن من خلالها مصداقية وحرص البنك، وفي ذات الوقت تحرص على عدم وضع العراقيل أمام التطور والابتكار، وعدم الإضرار بالوضعية التنافسية للبنوك في مقابل المؤسسات غير البنكية الضالعة في تقديم خدمات مصرفية على شبكة الإنترنت[٣].

---

(1) **Anita K. Pennathur**, Op. Cit, p. 2114.

(٢) راجع سابقا، ص ٧٦.

(٣) د. **سعيد الحامز**، مرجع سابق، ص ٢٣٩٥.

وفى ضوء ذلك جاء في التقرير السنوي للبنك المركزي المصري أنه يسعى إلى تطوير الوظيفة الرقابية بما يتماشى مع التطورات العالمية في الصناعة المصرفية، حيث تم البدء في استخدام أسلوب الرقابة عن طريق تقييم المخاطر، والتعرف على قدرة البنوك على تحديدها سواء الحالية أو المستقبلية وقياس تلك المخاطر ومتابعتها والرقابة عليها، وذلك بالإضافة إلى العمل على تأهيل البنوك لاتفاقية بازل الثانية بمطالبتها بالاهتمام بإدارات المخاطر بها، وإنشاء وحدات للتنبؤ وإدارة الأزمات والاهتمام بأسس الرقابة الداخلية(١).

وفى ضوء ما سبق، تم توقيع بروتوكول مع بعض الجهات الدولية (البنك الدولي، المجموعة الأوربية) للمساعدة الفنية لمدة عامين بهدف تطوير أدوات وأساليب الرقابة والإشراف، وتدريب الكوادر العاملة على استخدام الأدوات والأساليب الرقابية الحديثة(٢).

١١٢- وبعد أن عرضنا لأهم صور المخاطر التي يمكن أن يتعرض لها البنك الإلكتروني العامل عبر شبكة الإنترنت، والتي كشفت عن مساوئ عمل البنوك على شبكة الإنترنت، فإن الأمر قد يدفع للوهلة الأولى إلى التحذير من عمل هذه البنوك على شبكة الإنترنت، والاكتفاء بالعمل المصرفي التقليدي بعيدا عن هذه المخاطر ومشكلتها. لكن نرى ألا يحكم على الأمور من هذا المنظور الضيق بمعنى أن وجود بنوك تعمل وتؤدى خدماتها عبر شبكة الإنترنت ليس مجرد مظهر من مظاهر الترف الذي يمكن أن يتبناه مجتمع معين للتسهيل على

---

(١) **البنك المركزي المصري**، التقرير السنوي، ٢٠٠٤/٢٠٠٥، ص ٢٩.
Available at: http://www.cbe.org.eg/public/Annual%20Report%202005.pdf.

(٢) **البنك المركزي المصري**، التقرير السنوي، ٢٠٠٤/٢٠٠٥، مرجع سابق، ص ٢٩.

مواطنيه في الحصول على الخدمات المصرفية، ويعزف عنه آخر، لكن الأمر أصبح ضرورة لا غنى عنها لأي مجتمع (متقدم أو نام)[(١)].

فالبنوك الإلكترونية العاملة عبر شبكة الإنترنت تحتل وبحق مكان القلب من الجسد بالنسبة للتجارة الإلكترونية في عمومها، وذلك من خلال سيطرتها على نظم الدفع الإلكترونية، وهيمنتها على حركة التجارة عبر شبكة الإنترنت[(٢)]، الأمر الذي يدفعنا في هذا الصدد إلى تبني فلسفة فحواها جني الثمار وتجنب الإصابة بالأشواك[(٣)]، بمعنى أننا يمكن أن نحصد ثمار عمل البنوك عبر شبكة الإنترنت ــ والتي سبق ذكرها ــ وذلك إذا تم توفير سياج قانوني وأمني يكفل الوقاية من المخاطر وتداعياتها المختلفة إلى أقصى درجة ممكنة، ويضرب بعمق في وجود البنك على الشبكة، ويفرض غطاء على كل تعاملات البنك واتصالاته، سواء على مستوى التعامل بين العاملين على شبكة البنك الداخلية، أم على مستوى المتعاملين مع البنك من خلال شبكة الإنترنت. لكن لا يمكن للنظم القانونية والأمنية أن تحقق النتائج المرجوة دون وجود جهة رقابية تمهد الطريق وتنيره أمام هذه البنوك في بيئة الإنترنت الوعرة، وتأخذ بيده منذ اللحظة الأولى لتواجده في هذه البيئة، وذلك من خلال فرض مجموعة من الضوابط الرقابية على إنشاء وعمل هذه البنوك، تكون بمثابة الحد الأدنى من الضمانات لعمل هذه البنوك في ظل بيئة قانونية وأمنية محكمة.

---

(1) **G C Chalikias**; Op. Cit., p. 2.

(2) **Adrian McCullough and William Caelli**; Op. Cit., p. 338.

(3) **Ibid**,p 355.

المبحث الثاني

الضوابط الرقابية على البنك العامل عبر شبكة الإنترنت

١١٣- بعد أن تعرضنا في المبحث السابق لأهم صور المخاطر التي يمكن أن يتعرض لها البنك الإلكتروني العامل عبر شبكة الإنترنت، وأهم الأسباب التي تقف وراء حدوث هذه المخاطر، وتبين لنا كيف أن هذه المخاطر من شأنها أن تهدد بقاء البنك ووجوده على شبكة الإنترنت، فأن الأمر يفرض وجود إجراءات وقائية، تظهر في صورة ضوابط رقابية تسعى إلى تجنيب البنك هذه المخاطر، وتعفيه من تبعاتها المهلكة.

وتظهر الضوابط الرقابية في حياة البنك الإلكتروني العامل عبر شبكة الإنترنت على مرحلتين: المرحلة الأولى، عند إنشاء البنك على شبكة الإنترنت وقبل ممارسته لنشاطه، والتي تظهر في صورة حصول البنك على ترخيص من جهة الرقابة المختصة بممارسة العمل المصرفي على شبكة الإنترنت. والمرحلة الثانية، تظهر من خلال ممارسة جهة الرقابة لمجموعة من الإجراءات الرقابية على أثناء عمل هذه البنوك، الأمر الذي يدعونا إلى التعرف على تفاصيل كل مرحلة من أجل التوصل إلى رؤية واضحة لطبيعة العمل الرقابي في حياة هذه البنوك.

المطلب الأول

حصول البنك على ترخيص لممارسة العمل المصرفي على شبكة الإنترنت

١١٤- تجد الضوابط الرقابية طريقها إلى البنك الإلكتروني العامل عبر شبكة الإنترنت أول ما تجد من خلال ربط السماح للبنك بممارسة العمل المصرفي على شبكة الإنترنت بالحصول على ترخيص من جهة الرقابة يسمح له بذلك، حيث يكون هذا الترخيص بمثابة إشارة البدء للبنك بالعمل وتقديم خدماته. ولن تمنح جهة الرقابة مثل هذا الترخيص للبنك إلا بعد أن تتأكد من توافر كافة المتطلبات الرقابية التي يجب توافرها للترخيص لهذا البنك بالعمل.

١١٥- هذا وقد تواترت القوانين الخاصة بتنظيم البنك المركزي في مصر(١) (كجهة الرقابة على عمل البنوك في مصر)(٢) على النص على مجموعة من الشروط التي يجب توافرها في أي مؤسسة ترغب في ممارسة العمل المصرفي، حتى يرخص لها بذلك في مصر، والمطالع لهذه الشروط يلاحظ أن الهدف من تطلبها هو التأكد من قدرة المؤسسة طالبة الترخيص على تداول النقود وصناعة الائتمان، وذلك من خلال تقديم الخدمات المصرفية المختلفة.

والبنوك العاملة عبر شبكة الإنترنت لن يخرج دورها عن ذلك، الأمر الذي يجب معه التزام هذه البنوك بهذه الشروط ومن ثم، يجب التعرض ولو في عجالة

---

(١) مثل قانون البنوك والائتمان الصادر بالقرار بالقانون رقم ١٦٣ لسنة ١٩٥٧ والقانون رقم ١٢٠ لسنة ١٩٧٥ في شأن البنك المركزي المصري والجهاز المصرفي، والقانون ٨٨ لسنة ٢٠٠٣ الخاص بالبنك المركزي والجهاز المصرفي والنقد.

(٢) تنص المادة (٦) فقرة (د) من قانون البنك المركزي والجهاز المصرفي ٨٨ لسنة ٢٠٠٣ على أن "يتخذ البنك المركزي الوسائل التي تكفل تحقيق أهدافه والنهوض باختصاصاته، وله على الأخص: الرقابة على وحدات الجهاز المصرفي".

سريعة (حيث استفاضت المؤلفات العامة في عمليات البنوك في الحديث عنها) لمثل هذه الشروط.

الشرط الأول: قيد البنك الإلكتروني في سجل البنوك لدى البنك المركزي المصري:

نص المشرع المصري في المادة (٣١) من قانون البنك المركزي والجهاز المصرفي رقم ٨٨ لسنة ٢٠٠٣[1] على أن (يحظر على أي فرد أو هيئة أو منشأة غير مسجلة طبقا لأحكام هذا القانون، أن تباشر أي عمل من أعمال البنوك ويستثنى من ذلك الأشخاص الاعتبارية العامة التي تباشر عملا من هذه الأعمال في حدود سند إنشائها).

كما نص في المادة (٣٢) من ذات القانون على (أن يتم تسجيل أية منشأة ترغب في مزاولة أعمال البنوك في سجل يعد لهذا الغرض لدى البنك المركزي بعد موافقة مجلس إدارته).

ويتضح من هذا النص أنه لا يجوز للبنك الإلكتروني العامل عبر شبكة الإنترنت، والمنشأ وفقا لأحكام القانون المصري مزاولة عمليات البنوك إلا بعد القيد في السجل المعد لهذا الغرض لدى البنك المركزي المصري.

هذا وقد نصت المادة (٣٣) من ذات القانون على أن (يقدم طلب التسجيل إلى

---

(١) **قانون رقم ٨٨ لسنة ٢٠٠٣ بإصدار قانون البنك المركزي والجهاز المصرفي** والنقد. الجريدة الرسمية، العدد ٢٤ مكرر، ١٥ يونيه ٢٠٠٣ (السنة السادسة والأربعون).
Available at: http://www.cbe.org.eg/public/Law%20No.88%20for%202003.doc

البنك المركزي، طبقا للشروط والأوضاع التي تبينها اللائحة التنفيذية لهذا القانون..).

وقد جاء في هذه اللائحة[1]، أن يقدم صاحب الشأن أو من ينوب عنه طلب تأسيس البنك إلى الإدارة العامة للرقابة على البنوك بالبنك المركزي للحصول على موافقته بصفة مبدئية تمهيدا لاتخاذ إجراءات تأسيس البنك طبقا لأحكام القوانين المصرية.

وقد اشترطت هذه اللائحة أيضا أن يرفق بالطلب مجموعة مستندات توضح أسماء المؤسسين، وجنسياتهم، وعناوينهم، وحصص كل منهم في رأس المال المدفوع، ونسبة الأسهم التي ستطرح للاكتتاب على المصريين من الأشخاص الطبيعيين والاعتباريين، وبشرط ألا يقل ما يمتلكه المصريون عن ٥٢% من رأس المال[2]. بالإضافة إلى بيان باسم البنك وعنوانه ومركزه الرئيس، وغرضه، وقيمة رأس مال البنك وعدد الأسهم وقيمتها الاسمية، واشترطت أيضا أن يرفق بالطلب دراسة الجدوى الاقتصادية لإنشاء البنك؛ وما يفيد اختيار أحد المصريين مديرا عاما للبنك واسمه وعنوانه ومؤهلاته وخبراته. وأخيرا يجب أن يرفق بالطلب خطاب تعهد من أحد البنوك الأجنبية بضمان حقوق المودعين والدائنين في حالة زيادة حصة الشريك الأجنبي على ٥٠% من رأس المال المدفوع.

(١) وقد صدرت هذه اللائحة بقرار رئيس الجمهورية رقم ١٠١ لسنة ٢٠٠٤، منشورة بالجريدة الرسمية العدد ١٢ مكرر (أ) ٢٢ مارس ٢٠٠٤

(٢) تم إلغاء نسبة مشاركة غير المصريين في رؤوس أموال البنوك المشتركة والخاصة بموجب المادة ٢١ مكرر (١) من القانون رقم ١٦٣ ١٩٥٧ المضافة بالقانون ٩٧ لسنة ١٩٩٦.

وعن ما جاء بهذه اللائحة، وبخصوص البنك الإلكتروني يستعاض عن البيانات الخاصة باسم البنك وعنوانه في الطلب المقدم بالعنوان الإلكتروني للبنك على شبكة الإنترنت على أن يرفق بهذا الطلب ما يفيد تسجيل الاسم والعلامة التجارية للبنك، والعنوان الإلكتروني لدى الجهات المختصة بذلك(١).

ويخطر مقدم الطلب بالقرار الصادر في هذا الشأن خلال شهر من تاريخ تسليم الطلب مرفقا به المستندات المذكورة.

الشرط الثاني: الشكل القانوني للبنك الإلكتروني:

نصت المادة (٣٢) من القانون سالف الذكر على أن (يتم تسجيل أي منشأة ترغب في مزاولة أعمال البنوك في سجل خاص يعد لهذا الغرض لدى البنك المركزي بعد موافقة مجلس إداراته وطبقا للشروط الآتية:

أن يتخذ البنك أحد الأشكال الآتية:

أ - شركة مساهمة مصرية، جميع أسهمها اسمية.

ب- شخص اعتباري عام يكون من بين أغراضه القيام بأعمال البنوك.

ج- فرع لبنك أجنبي يتمتع مركزه الرئيس بجنسية محددة ويخضع لرقابة سلطة نقدية في الدولة التي يقع فيها مركزه الرئيس.

ووفقا لهذا النص فإن الشكل القانوني للبنك الإلكتروني لن يخرج عن ثلاثة فروض حتى يحصل على الترخيص وذلك على النحو التالي:

---

(١) انظر إجراءات تسجيل العلامة التجارية والعنوان الإلكتروني على شبكة الانترنت **د. شريف محمد غنام**، حماية العلامة التجارية في علاقتها بالعنوان الإلكتروني، مرجع سابق، ص ٧٧ وما بعدها.

<u>الشكل الأول</u> أن يؤسس البنك في صورة شركة مساهمة:

ولعل الحكمة التي تغياها المشرع من وراء اشتراط تأسيس البنك في هذه الصورة هو ما تتمتع به هذه الشركات من قدرة مالية وتنظيمية كبيرة، تعود إلى ما يسمح به نظامها القانوني من تقسيم رأس مالها في صورة أسهم، يتم الاكتتاب فيها من قبل الكافة. يضاف إلى ذلك أن شركات المساهمة عند تأسيسها، وأثناء مزاولة نشاطها تخضع لرقابة دقيقة من أجهزة الدولة(١)، وبناء عليه لا يجوز تأسيس البنك الإلكتروني في شكل آخر من أشكال الشركات التجارية (تضامن أو توصية بسيطة...)، بل من باب أولى يمتد الحظر للأفراد في طلب إنشاء البنك الإلكتروني في صورة منشأة فردية.

ووفقا للنص سالف الذكر لا يكفى لقيد البنك الإلكتروني أن تؤسسه شركة مساهمة، وإنما اشترط المشرع علاوة على ذلك أن تكون جميع أسهم هذه الشركة اسمية .وبذلك حظر المشرع صدور الأسهم لحاملها، ولعل الحكمة من وراء هذا الشرط هو فرض نوع من الرقابة على شخصية مالكي هذه الأسهم(٢).

<u>الشكل الثاني</u>: الأشخاص الاعتبارية العامة التي يكون من بين أغراضها القيام بعمليات البنوك:

ويلاحظ على النص أنه أتاح الفرصة للشخص الاعتباري العام إمكانية إنشاء البنك الإلكتروني على شبكة الإنترنت، بشرط أن يكون من بين اختصاصات هذا الشخص الاعتباري ممارسة عمليات البنوك، حتى وأن كان له اختصاصات

(١) **د. عبد الرحمن السيد قرمان**، عمليات البنوك، دار النهضة العربية، الطبعة الثانية، ٢٠٠٠، ص٢٣.

(٢) المرجع السابق، ص٢٥.

أخرى يمارسها بجانب عمليات البنوك:

الشكل الثالث: أن **يكون البنك الإلكتروني فرعًا لبنك أجنبي:**

أجاز المشرع إمكانية إنشاء البنك الإلكتروني من قبل **فرع لبنك أجنبـــي**، وذلك بشرطين:

١- أن يكون المركز الرئيس للبنك الأجنبي متمتعا بجنسية دولة معينة.

٢- أن يكون الفرع الرئيس للبنك الأجنبي خاضعا لرقابة سلطة نقدية في الدولة التي يقع فيها.

وهذا الفرض يمكن تصوره في خصوص البنك العامل عبر شبكة الإنترنت في حالة أن كان هناك أحد البنوك الأجنبية التقليدية (ليست الإلكترونية)، وترغب في إنشاء بنك إلكتروني في مصر يعمل على شبكة الإنترنت، كشكل مـــن أشـــكال الاستثمار في مجال الخدمات المالية، خاصة إذا كانت القوانين المصرية تمـــنح امتيازات، أو إعفاءات من شأنها أن تشجع مثل هذه البنوك علـــى إنـــشاء بنـــك إلكتروني لها وفقا للقوانين المصرية. وحسنا فعل المشرع المصري أنه لم يطلق الحبل على غاربه لهذه البنوك، بل قيد ذلك بقيود معينة، أراد مـــن ورائهـــا أن يستشف تمتع المركز الرئيس للبنك بضمانات تؤهله لممارسة العمل المـــصرفي في مصر، وذلك من خلال اشتراط تمتعه بجنسية دولة معينة، وخضوعه لرقابة سلطة نقدية في الدولة التي يقع فيها.

يضاف إلى ذلك قيدا أوردته المادة الخامسة مـــن القـــانون رقـــم ١٥٩ لـــسنة

١٩٨١[1] والذي حظر على شركات التوصية بالأسهم، والشركات ذات المسؤولية المحدودة القيام بأعمال البنوك، ومن ثم يجب ألا يكون البنك الأجنبي متخذا أحد هذه الأشكال القانونية، حتى يمكن أن يرخص له بالعمل كبنك إلكتروني في مصر.

الشرط الثالث: الحد الأدنى لرأس مال البنك الإلكتروني:

اشترط المشرع في المادة ٣٢ من القانون رقم ٨٨ لسنة ٢٠٠٣ أن يتوافر لدى المؤسسة التي تقوم بأعمال البنوك ألا يقل رأس المال المصدر والمدفوع بالكامل عن خمسمائة مليون جنيه مصري، وألا يقل رأس المال المخصص لنشاط فروع البنوك الأجنبية في جمهورية مصر العربية عن خمسين مليون دولار أمريكي أو ما يعادلها بالعملات الحرة[2].

وبناءً عليه، يجب أن يستوفى البنك الإلكتروني هذه النسبة من رأس المال حتى

---

(١) "لا يجوز أن تتولى شركات التوصية بالأسهم أو الشركات ذات المسؤولية المحدودة أعمال التأمين أو أعمال البنوك أو الادخار أو تلقى الودائع أو استثمار الأموال لحساب الغير". انظر **الجريدة الرسمية، العدد ٤٠، ١ أكتوبر سنة ١٩٨١**.

(٢) وهذا النص يختلف عن قانون البنك المركزي القديم في هذه الجزئية، حيث كان القانون القديم يشير إلى رأس المال بالمرخص به وبالمدفوع. فالمرخص به كان لا يقل عن مائة مليون جنيه مصري، والمدفوع لا يقل عن خمسين مليون جنيه، ويجوز سداده كليا أو جزئيا بالمعادل بالعملات الحرة.أما فروع البنوك الأجنبية فلا يقل رأس المال المخصص لنشاطها في مصر عن ١٥ مليون دولار أمريكي أو ما يعادله بالعملات الحرة. وقد غير القانون الجديد ذلك مطالبا جميع البنوك برفع رأسمالها إلى خمسمائة مليون جنيه مصري. ولم يفرق بين المرخص به والمدفوع بل تطلب أن يكون هذا المبلغ " مصدرا أو مدفوعا بالكامل ". وقد ظهر من تطبيق هذا النص أن البنك المركزي لا يشترط أن تضم الزيادة لرأس المال وتصدر مقابلها أسهم وإنما يكفى أن تقدم من المساهمين أو بعضهم كقروض متنازل عن مرتبتها subordinated debts وتخصص لاستيفاء معيار كفاية رأس المال. انظر د. **محي الدين إسماعيل علم الدين**، مرجع سابق، ص٦٢

يرخص له بالعمل. ولعل مثل هذا الشرط يعكس ضمانة قوية، تتمثل في الملاءة المالية التي تؤهل البنك الإلكتروني لمباشرة أعماله عبر شبكة الإنترنت (خاصة عمليات الائتمان)، وتطمئن المتعاملين معه على حقوقهم، وتزيدهم ثقة فيه.

الشرط الرابع: اعتماد البنك المركزي المصري للنظام الأساسي وعقود إدارة البنك الإلكتروني:

يشترط بالإضافة إلى ما سبق ذكره من شروط، شرط أخير نصت عليه المادة (٣٢) سالفة الذكر، وهو اعتماد البنك المركزي المصري لأمرين:

١)- النظام الأساسي للبنك. وهو العقد الخاص بتأسيس البنك، والذى ينظم طبيعة نشاطه، وأهدافه، وحقوق والتزامات المؤسسين، وغيرها [١].

٢)- عقود إدارة البنك الإلكتروني. ويقصد بها العقود التي يبرمها البنك الإلكتروني مع أي طرف يعهد إليه بإدارة البنك. وتزداد أهمية هذا الفرض في حالة إسناد إدارة البنك الإلكتروني المسجل في مصر إلى أحد الجهات الأجنبية[٢]، حيث ستزداد أهمية ممارسة نوع من الرقابة من قبل البنك المركزي على طبيعة هذه العقود، خاصة في ظل الأهمية الخاصة للنواحي الإدارية والتشغيلية في البنك الإلكتروني، الأمر الذي يلح في التأكد من جدية وكفاءة الإدارة ومدى تأهيلها الفني الذي يسمح لها بتسيير حركة العمل بدقة وكفاءة، سواء على صعيد العاملين على الشبكة الداخلية للبنك. أم على صعيد التعامل مع العملاء عبر شبكة الإنترنت، يضاف إلى ذلك أن إسناد

---

(1) **Sherif Mohamed Ghanam,** Banking Operations, Mansoura University- Faculty of Law. (without date publishment), p. 13.

(٢) د. **محي الدين إسماعيل علم الدين**، مرجع سابق. ص ٦٢.

مهمة إدارة أحد الكيانات الاقتصادية كالبنك العامل عبر شبكة الإنترنت أمر يحتاج إلى ممارسة نوع من الرقابة.

وبعد صدور الموافقة المبدئية من البنك المركزي على تأسيس البنك يبدأ أصحاب الشأن في اتخاذ إجراءات التأسيس؛ فإذا تمت على النحو المقرر قانونا، يقدم طلب تسجيل البنك إلي الإدارة العامة للرقابة على البنوك على النموذج المعتمد من محافظ البنك المركزي. ويرفق بهذا الطلب المستندات الآتية:

أ - الموافقة المبدئية على تأسيس البنك .

ب- القرار الصادر بتأسيس البنك.

جـ - صورة من عقد التأسيس والنظام الأساسي للشركة .

د - عقود الإدارة في حالة إبرامها مع أي طرف يعهد إليه بإدارة البنك.

هـ - صورة من محضر الجمعية العامة للشركة بالموافقة على تعيين أعضاء مجلس الإدارة، أو القرارات الصادرة بتعيين المديرين المسئولين الموكل إليهم إدارة أعمال فروع البنوك الأجنبية في مصر.

وبعد دراسة هذا الطلب يصدر مجلس إدارة البنك المركزي قراره إما بالموافقة وإما بالرفض.

وفي الحالة الأولى ينشر القرار في الجريدة الرسمية ويخطر أصحاب الشأن خلال ١٥ يوما من تاريخ صدوره؛ وبذلك يستطيع البنك مزاولة نشاطه. أما في حالة الرفض فيخطر الطالب بالقرار مع أسبابه بكتاب موصى عليه مصحوب بعلم الوصول خلال ١٥ يوما من تاريخ صدوره.

وإذا كانت الشروط سالفة الذكر شروطا عامة، وضعها المشرع المصري من أجل التأكد من توافر ضوابط وضمانات معينة تؤهل المؤسسة الراغبة في ممارسة عمليات البنوك من مواجهة المخاطر التقليدية المتعلقة بعمليات الائتمان وتداول النقود، فإن السؤال الذي يطل برأسه علينا هو إلى أي مدى راعى المشرع المصري طبيعة المخاطر المستحدثة في نظام عمل البنك الإلكتروني عبر شبكة الإنترنت، والتي سبق الحديث عنها؟

١١٦- في الواقع، المشرع المصري لم يصدر عنه حتى الآن تشريع خاص لمواجهة المخاطر المرتبطة بعمل البنوك الإلكترونية العاملة عبر شبكة الإنترنت، وذلك من خلال فرض شروط معينة ينبغي توافرها في البنك الإلكتروني العامل عبر شبكة الإنترنت حتى يرخص له بالعمل، الأمر الذي يشكل فراغا تشريعيا في واحدة من أهم المناطق حساسية وخطورة في نظام عمل هذه البنوك ويفرض بقوة ضرورة التدخل لرأب هذا الصدع، ومواجهة هذه التحديات.

وحسنا فعل البنك المركزي المصري- تفاديا لهذا الموقف الصامت من قبل المشرع المصري- حين أن أصدر مجموعة من الضوابط الرقابية، والتي تنطوي على مجموعة من الشروط يجب توافرها حتى يستطيع البنك أن يحصل على ترخيص لتقديم العمليات المصرفية الإلكترونية، وأهم هذه الضوابط هي[(١)]:

---

(١) **الضوابط الرقابية للعمليات المصرفية الإلكترونية وإصدار وسائل دفع للنقود الإلكترونية**، البنك المركزي المصري، الجلسة المنعقدة بتاريخ ٢٨ فبراير ٢٠٠٢، ص٢، متاحة على العنوان الإلكتروني التالي:

http://www.cbe.org.eg/public/Regulations%20of%20The%20Electronic%20Banking%20Operations.doc

(١) أن يتبع البنك مبادئ حصيفة لإدارة مخاطر تقديم خدماته من خلال شبكات الاتصال الإلكترونية، والتي تشتمل على تقييم المخاطر والرقابة عليها ومتابعتها.

(٢) أن يحدد البنك لدى طلبه للحصول على الترخيص نوعية الخدمات التي سيقوم بتأديتها من خلال الشبكات.

(٣) أن يحدد البنك المسؤوليات الواقعة عليه من جراء تقديم الخدمات عبر الشبكات.

(٤) أن يحدد البنك المسؤوليات الواقعة علي العميل جراء حصوله على الخدمات عبر الشبكات.

(٥) إفصاح البنك المرخص له بالقيام بالعمليات المصرفية الإلكترونية على صفحة web الخاصة به بما يفيد حصوله على ترخيص لتقديم خدماته عبر الشبكات، ورقم وتاريخ الحصول عليه، والخدمات التي يجوز للبنك تقديمها عبر شبكة الإنترنت، مع ربط هذا الموقع بصفحة البنك المركزي المصري المعلن فيها عن أسماء البنوك المرخص لها بذلك من خلال Hypertext Links[١] حتى يتحقق العملاء من صحة الترخيص.

١١٧- وفي ضوء تفصيل الشرطين الثالث والرابع من الشروط سالفة الذكر، فقد جاء في (المرفق رقم٢) من مذكرة الضوابط الرقابية للعمليات المصرفية

---

(١) وهي عبارة عن كلمة أو عبارة توجد في صفحة ويب معينة وتكون متصلة بنقطة أخري في ذات الصفحة، أو في صفحة أخرى، حيث بمجرد الضغط على هذه الكلمة أو العبارة يتم عرض الصفحة المتصلة بها. انظر:

Michael Chissick, Aslistair Kelman; Op. Cit, p. xxxix

الإلكترونية الصادرة عن البنك المركزي سالفة الذكر تفصيل للمسؤوليات الاسترشادية[1] للبنك عند تقديم خدماته عبر شبكات الاتصال الإلكترونية:

أ - موافقة مجلس إدارة البنك على إستراتيجية تتضمن قيام البنك بتقديم خدماته عبر الشبكات على أن يحاط المجلس بكافة المخاطر الناشئة عن ذلك.

ب- موافقة مجلس إدارة البنك على سياسة الإدارة التنفيذية للبنك فيما تتعلق بأسلوب إدارة المخاطر، وتدعيم نظم الرقابة الداخلية بشأن تلك المخاطر.

جـ - تصميم نماذج عقود لتأدية مختلف الخدمات المصرفية التي تؤدى عبر شبكات الاتصال الإلكترونية، وأن يتأكد البنك من توافر القوى البشرية المؤهلة للتعامل مع عملاء البنك عبر الشبكات. مع تحديد ساعات تقديم هذه الخدمات .

د - في حالة وجود طرف آخر تقدم من خلاله الخدمة، فيتعين على مجلس إدارة البنك إقرار اتفاقية التشغيل التي تنظم العلاقة بين البنك وهذا الطرف، مع تحديد مسئوليته في الحفاظ على سرية التعليمات والمعاملات التي تتم عبر الشبكات وأية معلومات تتاح له .

هـ - إفصاح البنك عن كون القوانين المصرية هي التي تحكم الخدمات التي يقوم بتأديتها للعملاء عبر الشبكات.

و - ضرورة أن يتحقق البنك من شخصية طالب/ متلقي الخدمة بأساليب قانونية

---

(١) جاءت هذه العبارة كما هي في نص الضوابط الصادرة عن البنك المركزي. ويبدو أن المقصود هو إرشادات لما يجب أن يقوم به البنك عند تقديم خدماته عبر شبكات الاتصال الإلكترونية.

ثابتة تضمن الحقوق المتبادلة.

١١٨- كما جاء في (المرفق رقم ٣) من ذات المذكرة تفصيل للمسئوليات الاسترشادية التي تقع على العميل عند تلقى خدماته عبر شبكات الاتصال الإلكترونية وهى[١]:

(أ) يتحمل العميل مسؤولية صحة المعلومات التي يقوم بإدخالها عبر الشبكات باعتباره مستخدما للخدمات التي تؤدى من خلالها، ويقر العميل بأن التعليمات والمعاملات التي يدخلها يتم التعامل عليها بدون أية مراجعة إضافية من البنك، أو إشعارات خطية أو التأكد منها بطرق أخرى.

(ب) لا يلتزم البنك بقبول أية تعديلات أو إلغاء تعليمات أو معاملات سبق أن أرسلها العميل عبر الشبكات.

(ج) يتحمل العميل مسؤولية إعداد البيانات الخاصة بالمستفيد أو الإضافة أو التعديل عليها.

(د) يلتزم العميل بمراعاة إجراءات الحماية في التعامل عبر الشبكات مع البنك.

(هـ) يتحمل العميل مسؤولية سوء استخدام الخدمة الناتج عن عدم الالتزام بإجراءات الحماية أو الشروط والأحكام الواردة في العقد الذي يتم إبرامه مع البنك بشأن العمليات المصرفية الإلكترونية، والناتج عن قيامه بالكشف عن إجراءات الحماية أو مخالفتها لدى الاستخدام .

(و) عدم تحمل البنك مسؤولية تعطل الخدمة لظروف خارجة عن إرادته.

---

(١) **الضوابط الرقابية للعمليات المصرفية الإلكترونية وإصدار وسائل دفع للنقود الإلكترونية**، المرجع السابق، ص١٠، ١١.

(ى) تعتبر سجلات البنك حجة قاطعة ملزمة قانونا على صحة المعاملات والتعليمات.

(ر) يلتزم العميل في حالة فقد أو سرقة جهاز الشفرة بإخطار البنك لكي يقوم بإبطال هذا الجهاز.

(ز) تعتبر أدوات الحماية وسيلة للتعرف والتحقق من شخصية العميل، وبمجرد إتمام إدخالها بنجاح يعتبر العميل هو مصدر جميع التعليمات والمعاملات.

١١٩- ويُحمد للبنك المركزي صنيعه في هذا الخصوص، فهي محاولة لا ينكر دورها في السماح للبنك المركزي كجهة رقابة في التأكد من توافر ضمانات معينة في المؤسسات التي تسعى لممارسة العمليات المصرفية عبر شبكة الإنترنت، سابقا على المشرع، الذي تأخرت خطاه كثيرا في وضع تنظيم قانوني يحكم وينظم عمل هذه البنوك والرقابة على نشاطها. وعلى الرغم من ذلك إلا أن هذه المحاولة من قبل البنك المركزي لا تعد كافية من وجهة نظرنا، وذلك لسببين:

الأول: يعود إلى إهمال العديد من الجوانب المكتظة بالمخاطر، والتي هي في أمس الحاجة إلى ضوابط رقابية تعمل على التأكد من تغطيتها، ويأتي في مقدمة هذه الجوانب؛ الجوانب الأمنية في حياة البنك الإلكتروني، والتي تعد وبحق من أكثر المناطق تعقيدا، وتلح في وجود تنظيم رقابي قوى وفعال لمواجهة هذه التعقيدات ذات الطبيعة الخاصة، والتي تجعل وجود البنك على شبكة الإنترنت مرهونا بالتصدي لها، أيضا من الجوانب التي أغفلها البنك المركزي تطلب وجود تأهيل فني مناسب سواء على مستوى إدارة البنك، أم على مستوى العاملين لديه. على الرغم من الأهمية القصوى لهذا الأمر، وعلى الرغم مما له من تأثيرًا

مباشر في تشغيل البنك على شبكة الإنترنت، يضاف إلى ذلك إغفال البعد الدولي لنشاط البنك الإلكتروني، وما يترتب على ذلك من تبعات على المستوى الرقابي. ويفرض مراعاة هذه التبعات وإيجاد آلية مناسبة للتعامل معها.

الثاني: ويتلخص في كون الجوانب التي شملها البنك المركزي بالتغطية ظهرت في صورة خطوط عريضة، مفتقدة التفصيلات التي من شأنها أن تعزز من الدور الرقابي، وذلك من خلال مزيد من التوضيح للمتطلبات الرقابية، وتطلب المزيد منها، وذلك على النحو الذي يحكم قبضة البنك المركزي في مواجهة هذه المخاطر. فعلى الرغم من أهمية الجوانب التي تعرض لها البنك المركزي، إلا أن الأمر كان يحتاج منه إلى عناية أكبر في صياغتها. فمثل هذه العبارات المتسعة تفتح الباب على مصراعيه للتأويل، ولا ترسم الحدود الرقابية المطلوبة بدقة.

١٢٠- وتبدو أهمية التعرض لأحد النظم الرقابية المقارنة بهدف تقييم الوضع في مصر والتأكد من مدى كفاية الضوابط التي صاغها البنك المركزي المصري في هذا الخصوص.

ففي الولايات المتحدة الأمريكية حظيت المخاطر المرتبطة بنشاط البنوك الإلكترونية العاملة عبر شبكة الإنترنت بعناية واهتمام مكتب الرقابة على النقد (OCC). فقد ربط منح الترخيص للبنك الإلكتروني للعمل وتأدية خدماته عبر شبكة الإنترنت بمجموعة كبيرة من الإجراءات الرقابية، يمر بها البنك عبر أطوار ومراحل متعددة، أراد من ورائها، وعلى ما يبدو أن يقلص إلى أقصى درجة ممكنة فرصة حدوث المخاطر المرتبطة بعمل هذا البنك بكافة أنواعها. لكن الملاحظ على هذه الإجراءات أن الكثير منها يهدف إلى مراعاة جوانب

اقتصادية ومحاسبية يشترك فيها البنك الإلكتروني مع غيره من البنوك الأخرى[١]، الأمر الذي يدفعنا إلى تسليط الضوء فقط على ما يتعلق من هذه الإجراءات بالجوانب المستحدثة في إنشاء وتشغيل البنك على شبكة الإنترنت.

١٢١- وقد تناول مكتب الرقابة على النقد هذه الإجراءات على النحو التالي[٢]:

١)- يجب ألا يقل التقسيم الأولى لرأس مال البنك، وتكاليف إنشاء الشبكة الإلكترونية الداخلية له، وجميع النفقات التنظيمية وقبل الافتتاحية عن ١٧,٥ مليون دولار. وقد برر مكتب الرقابة على النقد هذا المبلغ، بأنها النسبة الكافية لدعم إنشاء البنك وتشغيله على شبكة الإنترنت. من ذلك أيضا تأهيل البنك لاستيعاب الحجم المتوقع من الصفقات والعمليات المصرفية. وعلاوة على ذلك ضرورة مراعاة وجود دعم مالي مناسب لتنفيذ خطة الطوارئ الملحقة بخطة التشغيل في حالة أن دعت الظروف لإعمالها.

٢)- يجب على البنك الإلكتروني أن يستوفى جميع الإجراءات الموضوعة من قبل مكتب الرقابة على النقد (OCC) للمراجعة والموافقة على نظام تشغيل البنك، سواء فيما يتعلق بالتصميم الفني للشبكة الإلكترونية للبنك، أو برامج

---

(١) فمثلا يشترط هذا المكتب حتى يرخص للبنك الإلكتروني بالعمل أن يقدم خطة لتشغيل البنك تفيد مراعاته لما نصت عليه مجموعة قوانين إعادة الاستثمار (Community Reinvestment Act) وتعليماته المرتبطة بهذه القوانين. وأيضا بيانا بالنفقات المتوقع إنفاقها، والأرباح المتوقع تحقيقها من وراء نشاط البنك، قوائم بمرتبات العاملين، ورسوم التأمين.

Decision of the office of the comptroller of the currency on the application to charter, Conditional Approval (347), January 2000, p. 4-5.

(2) **Ibid**, p. 14.

المعلومات القائمة على تشغيل هذه الشبكة. ويجب أن يضمن البنك ضمن أوراقه رسما تخطيطيا وشرحا وافيا لكل العناصر الداخلة في تكوين هذه الشبكة، بما في ذلك المواقع الإلكترونية التي يوجد لها رابط (Hypertext) على موقع البنك على شبكة الإنترنت (كالتجار الذين يعلنون عن منتجاتهم على موقع البنك)، والعقود التي تحكم علاقة البنك بهؤلاء التجار[1]، بالإضافة إلى العقود الخاصة بتأمين الشبكة الداخلية والموقع الإلكتروني للبنك.

٣)- يجب على البنك أن يستوفى جميع الإجراءات الموضوعة من قبل مكتب الرقابة على النقد (OCC)، للمراجعة والموافقة على السياسة الائتمانية التي سوف يتبعها البنك في تعاملاته مع العملاء؛ بما في ذلك نظام الإقراض، وأنواع القروض وحجمها، وأنواع الضمانات التي سيتطلبها البنك من العملاء لمنح هذه القروض.

٤)- يجب على البنك أن يقدم لمكتب الرقابة على النقد ما يفيد استيفاءه لكل المتطلبات الأمنية، سواء فيما يتعلق بالأجهزة والأدوات الخاصة بتأمين وجود البنك وتعاملاته، أم فيما يتعلق بالإجراءات التي سيفرض البنك التعامل بها مع أجهزته من قبل كل من العاملين لديه أو المتعاملين معه، كذلك يجب أن يقدم ما يفيد اختبار تشغيل هذه الأجهزة من قبل مراجع فني متخصص في هذا المجال، ويجب على هذا المراجع أن يعد تقريرا مكتوبا

---

(١) ويعد هذا العقد من قبيل عقود الإيواء، والتي يكون البنك الإلكتروني فيها هو المستضيف. ويسري على هذا العقد ذات الأحكام التي سبق تناولها في عقد الإيواء. انظر سابقا ص ١٧٩.

(Written Report)، يدون فيه أنواع التدابير الأمنية التي استعان بها البنك، بما في ذلك برامج الحماية، والإجراءات الخاصة بالتحكم والتأكد من البيانات الداخلة والخارجة، ونظم التحقق من شخصية المتعامل مع البنك، والإجراءات التي تكفل الدخول الآمن على الموقع الإلكتروني للبنك والتعامل معه، حيث يقوم المكتب بعد ذلك بإجراء فحص أمني شامل (comprehensive security review) لهذه العناصر، وذلك لتقييم الاستعداد الأمني من قبل البنك في ضوء المخاطر المرتبطة بنشاطه، خاصة المخاطر الناجمة عن استخدام التكنولوجيا. ويملك مكتب الرقابة على النقد أن يبدى أي ملاحظات أو توصيات تتعلق بهذا الاستعداد الأمني، وله أن يؤخر إصدار القرار النهائي بالموافقة على الترخيص للبنك، حتى يتأكد تماما من إنجاز كل هذه الملاحظات والتوصيات كما طلب، فإن لم يتم استيفاؤها على الرغم من كل هذا فله أن يرفض الطلب.

ه)- يجب على البنك أن يقدم لمكتب الرقابة على النقد ما يفيد تأهيل الطاقم الإداري سواء على مستوى المدراء أم على مستوى العاملين.

هذا وقد أوضح مكتب الرقابة المقصود بهذا التأهيل، من خلال ربط هذا المعنى بأمور معينة، وهي:

أ - العلم والدراية الكافيين بالقوانين الوطنية المتعلقة بالبنوك.

ب- امتلاك خبرة قوية في تنظيم تقديم العمليات المصرفية الإلكترونية عبر شبكة الإنترنت؛ خاصة ما يتعلق بأنواع هذه العمليات وتصنيفها وكيفية تقديمها، وذلك في ضوء الحجم المتوقع (projected volume) تقديمه

من قبل البنك المراد إنشائه.

ج - القدرة على تحقيق ربحية معقولة من خلال إدارة البنك، والحفاظ على ذلك.

د - الخبرة الكافية في التعامل مع الأجهزة الإلكترونية المصرفية وبرامجها المتخصصة.

وقد شدد المكتب على العنصر الأخير؛ وذلك لارتباطه المباشر بعمل البنك وتشغيله، بل تطلب علاوة على ذلك تخصيص وحدات إدارية تختص بنظم تكنولوجيا المعلومات، على أن ينصب على رأس هذه الوحدات أفراد للعمل كمديرين لمهندسي التكنولوجيا. ويجب أن يكون لدى هؤلاء الأفراد مهارات قيادية(leadership skills) بشؤون الكمبيوتر والإنترنت، وذلك على النحو الذي لا يمكنهم فقط من إدارة وتشغيل البنك على شبكة الإنترنت، ولكن أيضا امتلاك القدرة على تفهم الاحتياجات المتجددة للنشاط المصرفي، وذلك على النحو الذي يجعل نشاط البنك مستوعبا لكل أشكال التطور بصورة مستمرة. ويعتبر هؤلاء موظفين تنفيذيين كبارًا (senior exécutive officiers) وفقا للأغراض الموضحة في القانون 12 C.F.R part 5 (١)، كما يجب على البنك أن يراعى التأهيل الفني لجميع العاملين لديه، حتى أصحاب التخصصات المحاسبية والمالية.

ولمكتب الرقابة على النقد (OCC) أن يتأكد من تأهيل هؤلاء الأفراد، وألا

(١) يرمز اختصار (CFR) إلى كود القوانين الفيدرالية الأمريكية (Code Federal Regulation)، ويختص القسم الثانى عشر الباب الخامس منه بالقوانين المتعلقة بالبنوك وتعاملاتها المصرفية. وهذا القانون متاح على العنوان الإلكتروني التالى:
http://www.occ.treas.gov/fr/cfrparts/12cfr05.htm

يكون لديه أي اعتراض عليهم، وذلك من خلال الاطلاع على مؤهلاتهم، وإجراء مقابلات شخصية- خاصة على مستوى المدراء- للتأكد من تـأهيلهم وقـدراتهم على تشغيل البنك عبر شبكة الإنترنت.

٦)- يجب أن يقـدم البنـك خطـة تـشغيل احتياطيـة لمواجهـة الطـوارئ (contingency plan)(١)؛ وذلك لمواجهة الأحداث الطارئة التي يمكن أن تقع أثناء عمل البنك، والتي يكون من شأنها أن تؤثر على انتظام سير العمل المصرفي. وقد وضح المكتب المقصود بالأحداث الطارئة، بأنها الأحـداث ذات البعد الاقتصادي؛ كحدوث تقلبات شديدة في عمليـات الإقـراض، أو ارتفاع نفقات التشغيل، والأحداث ذات البعد فني، كحدوث أعطال مفاجئـة في الأجهزة والمعدات العاملة على شبكة البنك، أو حدوث اختـراق أمنـي لنظم معلومات البنك. ويجب أن تكون هذه الخطة متوافقة مع تعليمات مكتب الرقابة على النقد (OCC)، وتكون قائمة على أسس سليمة، وتوفر حلـولاً بديلة وسريعة لمواجهة هذه الأزمات، وتنظم اللجوء لرأس المال الاحتياطي لمواجهة التقلبات الاقتصادية، أيضا تـنظم كيفيـة الاسـتعانة بـالأجهزة الإلكترونية البديلة في حالة حدوث أعطال فنية، وذلك على النحو الذي يمكن

(١) وقد أظهرت الدراسات الأهمية القصوى لخطة الطوارئ فـي نظـام عمـل البنـك الإلكتروني العامل عبر شبكة الانترنت. وتكمن هذه الأهمية من تأكيدها علـى قـدرة البنك على الاستمرار في التواصل مع عملائه وتقديم الخدمات المصرفية لهم، حتـى في أعتى الظروف. فالاعتماد الكبير من جانب البنـك علـى الوسـائل الإلكترونيـة وملحقاتها من البرامج المختلفة، من شانه أن يثير بعض القلق، سواء من ناحية سلامة هذه الأشياء وانتظامها في العمل، أم من ناحية قابليتها للانتهـاك الأمنـي لاتـصالها المباشر بشبكة دولية للاتصال عن بعد، الأمر الذي يعظم من دور خطة الطوارئ في حياة البنك، والتي تقدم الحل البديل السريع لمواصلة تفاعل البنك مع عملائه.

Internet Banking; Op. Cit, p. 8.

البنك من مواصلة العمل، والتغلب على مثل هذه الأمور.

٧)- يجب على البنك أن يقدم أيضا خطة للرقابة الداخلية، توضح تبنى البنك نوع من الرقابة الذاتية على مجمل نشاطه، سواء على مستوى العاملين لديه (في مختلف التخصصات)، أم على مستوى التعامل مع العملاء. ويجب أن تتضمن هذه الخطة تخصيص إدارة تقوم على هذا الأمر وفق إجراءات دقيقة ومحكمة، من شأنها أن تعكس رؤية واضحة تجلى للبنك أموره وتحيطه علما بكل شؤونه على كافة الأصعدة.

١٢٢- وبعد أن يستوفى البنك كل هذه الإجراءات فإن موقف مكتب الرقابة على النقد (OCC) سيتراوح بين ثلاثة أحوال على النحو التالى[1]:

(١) <u>الموافقة الأولية (**preliminary approval**)</u>: تشير إلى الترخيص للبنك في اتخاذ الخطوات اللازمة للإنشاء الفعلي للبنك طبقا للخطة المبينة في الطلب، وهذه الخطوات تشتمل على انتقاء العاملين وفقا للضوابط المقررة من قبل مكتب الرقابة على النقد، وشراء كافة المكونات المادية والمعنوية اللازمة لإنشاء وتشغيل البنك، وغيرها من الخطوات المتطلبة، والموافقة الأولية بهذا المعنى لا تعنى ترخيصا نهائيا للبنك ببداية ممارسة العمل المصرفي، ولكنها مجرد تصريح للبدء في إنشاء البنك، تحتاج إلى موافقة نهائية من قبل مكتب الرقابة، بعد أن يتأكد تماما من استجماع البنك لكل المتطلبات الرقابية. لكن هذه الموافقة تفيد استيفاء الطلب المقدم من البنك

---

(1) **Decision of the office of the comptroller of the currency on the application to charter**, Conditional Approval (347), Op. Cit, p. 13.

لكل العناصر المطلوبة، وذلك على النحو الذي يدفع مكتب الرقابة على النقد للسماح له بالسير في الإجراءات طبقا للطلب المقدم.

وبمجرد أن يمنح مكتب الرقابة على النقد (OCC) الموافقة الأولية للترخيص المقترح، فإن المجموعة المنظمة يجب عليها أن تنجز المتطلبات الإجرائية الأساسية، وفى بعض الحالات المتطلبات الخاصة قبل أن يمنح المكتب الموافقة النهائية، بالإضافة إلى أن المكتب قد يفرض شروطا تظل سارية حتى بعد فتح البنك.

(٢) <u>الموافقة الأولية المشروطة preliminary conditional approval)</u>: وهى موافقة تصدر متضمنة بعض المتطلبات قبل الافتتاح (preopening requirement)، وشروطا مستمرة (on-going conditions) بعد الافتتاح، بمعنى أن مكتب الرقابة يوافق للبنك على البدء في اتخاذ إجراءات الإنشاء، لكن وفقا لمتطلبات معينة يحددها المكتب في تصريحه، ويتخذ شروطا تظل مفروضة على البنك أثناء تشغيله.

وهذه الحالة تعكس على ما يبدو عدم استيفاء الطلب المقدم من قبل البنك لبعض المتطلبات الرقابية الثانوية المفروضة من قبل مكتب الرقابة على النقد (OCC)، والتي يمكن منح الموافقة للبنك بالبدء في اتخاذ الإجراءات، ولكن بشروط معينة.

(٣) <u>الرفض (disapproval):</u> وقد جاء في الدراسة الصادرة عن مكتب الرقابة (OCC) ذكر لحالة الرفض كأحد المواقف التي يمكن أن يتخذها المكتب حيال الطلب المقدم من قبل البنك، ولكن لم يوضح الأسباب التي

تبرر لجوءه لرفض الطلب المقدم من قبل البنك. لكن يمكن القول بأن الرفض يكون نتيجة لعدم استيفاء الطلب المقدم من قبل البنك للمتطلبات الأساسية والجوهرية التي يمكن معها السماح للبنك باتخاذ إجراءات الإنشاء. بمعنى آخر الطلب المقدم من قبل البنك لم يحز على الحد الأدنى من المتطلبات اللازمة، الأمر الذي يدفع مكتب الرقابة على النقد لرفض هذا الطلب.

١٢٣- وفي النهاية، بعد عرض المتطلبات الرقابية لكل من البنك المركزي المصري ومكتب الرقابة على النقد الأمريكي، نلاحظ أنها جميعها تنهل من معين واحد، وهو محاولة تفادى أو حتى التقليل قدر المستطاع من المخاطر التي يمكن أن يتعرض لها البنك الإلكتروني العامل عبر شبكة الإنترنت، ومن ثم عملاؤه. وذلك على النحو الذي يوفر مناخا خاليا من المخاطر، ويحقق الاستقرار في المعاملات المصرفية التي تتم عبر هذه الشبكة. لكن هذا لا يجعلنا نساوى تماما بين موقف كل منهما: فمكتب الرقابة على النقد (OCC) استطاع أن يتفادى الانتقادات التي سبق أن وجهت للبنك المركزي المصري، وذلك من خلال التطرق تقريبا لكل نقاط الضعف التي يمكن أن تشكل مصدرا لتهديد وجود البنك وتشغيله على شبكة الإنترنت، بل ووضع إجراءات دقيقة ومحكمة لمواجهة هذه التهديدات، بل أنه لم يغفل وجود حالات طوارئ مفاجئة يمكن أن تهدد وجود البنك فتطلب لذلك خطة طوارئ توفر حلولا بديلة في حالة تعرض البنك لمخاطر لم تكن ظاهرة على نحو يوفر مزيدا من التأمين والاستمرارية في عمل البنك، يضاف إلى كل ذلك أنه لم يجعل موافقته على الطلب المقدم من قبل البنك موافقة نهائية، إلا بعد أن يتأكد تماما وبصورة فعلية من أنجاز البنك لكل المتطلبات

المفروضة، الأمر الذي يعكس إدراكه لمدى خطورة التهديدات التي تحيط البنك وعمله، واهتمامه بحصرها، وذلك من خلال مجموعة من الإجراءات المنطوية على العديد من الشروط التي تهدف في النهاية إلى تهيئة البنك للإنشاء والعمل عبر شبكة الإنترنت.

١٢٤- الأمر الذي يدعونا إلى توجيه النداء العاجل للبنك المركزي المصري إلى ضرورة تبنى صيغة جديدة للضوابط التي سبق أن وضعها (بتاريخ ٢٨ فبراير٢٠٠٢)، صيغة تعكس إدراكا أكبر لطبيعة وحجم المخاطر التي تلوح في أفق البنك الإلكتروني العامل عبر شبكة الإنترنت، وذلك من خلال إعداد دراسة شاملة تهدف إلى ولوج كل المناطق الخطرة في نظام عمل البنك، وتحديد مدى تأثيراها عليه، ووضع إجراءات دقيقة ومفصلة تهدف إلى إخلاء ساحة البنك من هذه المخاطر، وتمهد له الطريق للسير بأمان وبخطى ثابتة.

١٢٥- لكن هذا لا يمنعنا من توجيه النقد لمكتب الرقابة على النقد الأمريكي في أمرين:

(١) إغفاله فرض ضوابط رقابية على العلاقة التي تجمع البنك بمزودي الخدمات الإلكترونية المختلفة، خاصة التي تلعب دورا كبيرا في وجود البنك وتشغيله على شبكة الإنترنت، مثل مقدم خدمة الدخول ومتعهد الإيواء، وحرصه على إلزام البنك من خلال ضوابط صارمة للتأكد من التراخيص التي تسمح لهؤلاء بتقديم خدماتهم، والنظر في التعاقدات التي تحكم علاقتهم بالبنك، ومدى ملاءمتها في ضوء الالتزامات، والمسؤوليات الواقعة على أطرافها.

(٢) عدم مراعاته للمخاطر الناجمة عن دولية نشاط البنك الإلكتروني العامل عبر شبكة الإنترنت، خاصة ما يتعلق منها بالبنوك الكائنة في دولة ما وتؤدى

خدمات داخل الولايات المتحدة الأمريكية، ومدى التأكد من صلاحية هذه البنوك لمباشرة العمليات المصرفية من عدمه، الأمر الذي يظهر لنا أهمية وجود شكل من أشكال التعاون الدولي للتصدي لهذا الخطر العضال الذي تعجز الجهود الفردية عن مواجهته (وقد كان هذا هو موقف البنك المركزي المصري أيضا)، الأمر الذي تلح معه الحاجة إلى اتفاقية دولية تعقد تحت مظلة أحد المنظمات العالمية (منظمة الأمم المتحدة) تشتمل على أسس ومعايير دقيقة، ذات طابع ملزم، تهدف إلى مواجهة هذه المخاطر بصورة جماعية.

المطلب الثاني

الإجراءات الرقابية أثناء عمل البنك الإلكتروني

١٢٦- سبق أن تعرضنا للمرحلة الرقابية الأولى في حياة البنك الإلكتروني العامل عبر شبكة الإنترنت، ورأينا مدى أهمية هذه المرحلة في حياة البنك؛ حيث تشهد الخطوات الأولى لإنشائه، وتسعى إلى وضع هذه الخطوات على الطريق الصحيح والآمن، من خلال تطلب مجموعة من الضوابط الرقابية يجب أن

يستوفيها البنك ليرخص له بالإنشاء والعمل. لكن هذه المرحلة تتسم بأنها مرحلة وقتية تنتهي بمجرد استكمال البنك لبنيانه، الأمر الذي تظهر معه الحاجة إلى مرحلة رقابية أخرى تمتد طوال فترة عمل البنك، تبررها وتعزز من وجودها استمرارية المخاطر وتجددها في حياة هذا البنك، بما تظهر معه الحاجة إلى الاستمرارية في الرقابة على عمله(١).

ويقصد بالاستمرارية في الرقابة على عمل البنك، تبني جهة الرقابة لمجموعة من الإجراءات الرقابية الدورية، بمواعيد ثابتة ومفاجئة، وذلك على النحو الذي يضمن لها تقيد البنك أثناء ممارسته لنشاطه بالمعايير الرقابية، والتي من شأنها أن تكفل له الاستمرار في العمل بشكل آمن وفعال، وتحمي المتعامل معه من المخاطر المرتبطة بنشاطه(٢).

لكن ما هي الإجراءات الرقابية التي يخضع لها البنك من قبل جهة الرقابة أثناء مباشرته لنشاطه على شبكة الإنترنت؟

١٢٧- يمكن القول، للوهلة الأولى، أن إجراءات الرقابة لن تبتعد عن التنقيب في أهم المناطق خطورة في نظام تشغيل البنك (المخاطر الأمنية، المخاطر القانونية، المخاطر التشغيلية)، لترى إلى أي مدى التزام البنك بالاحتياطات الكافية لمنع تسرب هذه المخاطر إلى ساحاته أثناء مباشرته لنشاطه، ومدى كفاية هذه الاحتياطات وتناسبها مع حجم ونوعية هذه المخاطر، ومدى تطوير البنك من هذه الاحتياطات على النحو الذي يجعلها قادرة على مجابهة التحويرات في أشكال

---

(1) **Anita K. Pennathur**; Op. Cit, p. 2116; **Apostolos Ath. Gkoutzinis**;Op. Cit., p. 20.

(2) **Internet Banking**; Op. Cit, p. 22.

المخاطر. وبناء عليه سوف تستهدف هذه الإجراءات مراعاة الجوانب الأمنية، والقانونية، والتشغيلية، وذلك على التفصيل التالي:

أولا- التأكد من استمرار كفاية وجودة المعايير الأمنية:

١٢٨- تأتى المعايير الأمنية دائما في مقدمة كل دراسة تتناول المخاطر المتعلقة بالبنك الإلكتروني عملياته علي شبكة الإنترنت[١]. لكن الحديث هذه المرة يستهدف التأكد من مواصلة البنك التزامه بهذه المعايير (والتى سبق أن التزم بها عند الإنشاء)، ومراعاته لتحديثها وفقا لما يستجد من مخاطر أمنية، والحرص على أن تأتى هذه المعايير ملائمة لهذه المخاطر كما وكيفا. وفى سبيل ذلك تعمل جهة الرقابة على التأكد من نقاط معينة، وذلك على النحو التالى[٢]:

١) التأكد من التزام البنك بالسياسة الأمنية التي تبناها عند بداية إنشائه، سواء فيما يتعلق بأمن الشبكة الداخلية للبنك أم فيما يتعلق بالموقع الإلكتروني له، والنظر في مدى ملاءمة هذه السياسة لطبيعة عمل البنك وقت إجراء الرقابة؛ وذلك كما لو كانت هناك بعض التوسعات التي أجرها البنك في نشاطه (كما لو استحدث أنشطة مصرفية جديدة)، أو إجراء تعديلات في هذا النشاط، الأمر الذي قد يؤدى إلى وجود إجراءات أمنية إضافية، ومن ثم يحتاج إلى مراجعة من قبل جهة الرقابة للتأكد من كفاية هذه الإجراءات بما يتلاءم مع طبيعة هذه التوسعات.

---

(1) **Apostolos Ath. Gkoutzinis,** Op. Cit, p. 149; **John Carlson, Karen Furst, William W. Lang, Daniel E. Nolle**; Op. Cit, p. 20.

(2) **Internet Banking**; Op.Cit,p. 29: **Decision of the office of the comptroller of the currency on the application to charter**; Conditional Approval 347,Op.cit, P 15.

٢) إجراء فحص دقيق لكافة مداخل ومخارج البيانات الخاصة بالبنك، وذلك للتأكد من استمرار عمل الوسائل الأمنية المسئولة عن سلامة هذه البيانات وتكاملها، كمرشحات البيانات (Filters Packet)، وبوابات التحكم (Gateways control)[1]، بالإضافة إلى البرامج الخاصة بالحماية ضد الفيروسات، وذلك من خلال اختبار عمل هذه الوسائل والتأكد من كفايتها لحجم البيانات الداخلة والخارجة من البنك وإليه.

٣) إجراء فحص دقيق لكافة الأدوات الأمنية المسئولة عن سرية البيانات الخاصة بالبنك وعملائه، والتأكد من التزام البنك بتفعيل كافة نظم التشفير (Encryption) وتحديثها، الأمر الذي يجعلها دائما مستعصية على الكشف، وذلك من خلال اتباع وسائل آمنة في إدارة المفاتيح الخاصة بعمليات

---

(١) وتعمل **مرشحات البيانات** على فحص كل حزمة بيانات قادمة أو خارجة كي يتم التعرف على مدى مطابقتها للقواعد الحاكمة لنظام العمل على شبكة البنك الإلكتروني، وذلك كما لو كانت القواعد التي تحكم الدخول على موقع البنك الإلكتروني تمنع دخول أي حزم بيانات محملة ببرامج تعمل على تدمير الموقع أو سرقة ما به من بيانات، ومن ثم تقوم مرشحات مجموعة البيانات في هذه الحالة بمنع مثل هذه الحزم من الدخول.

- وتعمل **بوابات التحكم** بذات عمل مرشحات البيانات. فهي أيضا تقوم بالحجب الكلي للعناوين الداخلية للبنك الإلكتروني، بحيث لا ترى الجهات الخارجية إلا الصفحة الرئيسة لموقع البنك الإلكتروني، على نحو تظهر معه كافة تعاملات البنك الإلكتروني بعنوان الصفحة الرئيسة لموقع البنك الإلكتروني فقط، ومن ثم تمنع أي محاولة خارجية للنفاذ إلى المكونات الداخلية لموقع البنك الإلكتروني، كما تعمل أيضا على التحكم في الأدوات الأمنية لكافة التطبيقات الخاصة بالعمليات المصرفية حتى تسمح فقط للأطراف الشرعيين أو المخول لهم (authorizedparties) بالدخول إلى هذه التطبيقات.

انظر. رأفت رضوان، مرجع السابق، ص١٠٩

Thomas C. Glaessner, Tom Kellermann, Valerie McNevin; Op, Cit., p. 69.

التشفير، وتشغيلها وإلغائها، وتخزينها لحماية سريتها. ويكون البنك دائما هو المسئول الأول قانونا في مواجهة العملاء عن أي إخلال يمس سرية هـذه البيانات[١].

٤) التأكد من بسط البنك سيطرته الكاملة على الدخول إلى موقعه الإلكتروني، وذلك من خلال فحص واختبار وسائل وأدوات التحكم في الدخول، والتي تسمح بالتعرف على شخصية المتعامل مع البنك، وتحديد هويته، والتي من أهمها نظام كلمات المرور (Password)، والوسائل المعتمدة على الخواص البيومترية[٢] (مثل بصمة الأصابع، اتساع حدقة العين، درجة تردد الصوت) والتي لا تسمح بالدخول إلا لمن له الحق في ذلك، وتمنع كل صور الدخول غير المشروع (unauthorized access).

٥)- التأكد من التزام البنك باتباع إجراءات دقيقة فيما يتعلق بتوثيق معاملاته[٣]، وذلك من خلال النظر في مدى اعتماد البنك على نظام التوثيق في تعاقداته مع عملائه، من خلال تطلبه حصول العميل على شهادة توثيق من جهة

---

(1) **John Carlson, Karen Furst, William W. Lang, Daniel E. Nolle**; Op. Cit., p. 18.

(٢) وأهم ما تتميز به هذه الوسائل أنها مرتبطة بشخصية عميل البنك، وذلك على النحو الذى لا يسمح لغيره باستعمالها، وذلك على عكس كلمة المرور التي يمكن لغير عميل البنك استعمالها.

Identity theft and identity fraud, available at: http://www.usdoj.gov/criminal/ fraud/websites/idtheft.html

(3) **Jon M. PEHA**, Electronic commerce with verifiable audit trails, available at: http://www.chicagofed.org/consumer_information/what_you_should_know_about_internet_banking.cfm; http://www.ece.cmu.edu/~peha/etrans.html

معتمدة تفيد تمتع هذا العميل بالأهلية القانونية اللازمة لمباشرة التصرفات القانونية، وصحة الإرادة الصادرة عنه، وتزويد العميل بمفاتيح التشفير اللازمة، وذلك قبل **دخوله في أي معاملة مصرفية معه**(١).

٦)- التزام البنك بخطة الطوارئ الخاصة به، والتأكد من تفعيله لها على نحو صحيح، والنظر في مدى ملاءمة هذه الخطة لحال البنك وقت الرقابة، وذلك من حيث كفاية الإجراءات التي تنظمها مع طبيعة عمل البنك، والتطورات التي أدخلت على نشاطه.

٧)- التأكد من التزام البنك بتفعيل نظم الرقابة الداخلية على كافة الأنشطة التي تتم داخل البنك(٢)، سواء على مستوى العاملين لدى البنك عبر الشبكة الداخلية له، أم على مستوى العملاء والتي تتم عبر موقعه الإلكتروني على شبكة الإنترنت(٣). ويجب أن يعد البنك تقارير مكتوبة عن نشاط الرقابة الداخلية له، وذلك حتى تكون تحت سمع وبصر جهة الرقابة عند إجراء الفحص الدوري لها(٤). ويجب أن تنطوي هذه التقارير على قدر كبير من الشفافية والمصداقية، على النحو الذي تساهم به في رسم رؤية واضحة عن حال النظم الأمنية الخاصة بالبنك، ومدى كفايتها وفاعليتها في حماية مقدرات البنك، وعلى جهة الرقابة أن تتأكد من ذلك جيدا، وذلك من خلال

---

(1) **Authentication in an electronic banking enviroment,** August 2001, available at: http://www.cdt.org/privacy/eudirective/EU_Directive_.html

(2) **Carl Pacini and others**; Op. Cit, p. 189.

(3) **Anita K. Pennathur**;Op. Cit, p. 2111.

(4) **Is auditing guideline internet banking**; Op. Cit., p. 3.

مراجعة هذه التقارير ومناقشتها مع المختصين، وذلك للتأكد من صحة ما جاء بها.

ثانيا- التزام البنك بالقوانين الحاكمة للعمل المصرفي على شبكة الإنترنت:

١٢٩- سبق الحديث عن أهمية الرقابة على مدى التزام البنك العامل عبر شبكة الإنترنت بالقوانين والتشريعات التي تحكم وتنظم عمل هذه البنوك، ورأينا كيف أن شبكة الإنترنت كبيئة يحيا فيها البنك ويتفاعل مع مكوناتها عكست تحديات قانونية أثارت ولا تزال تثير العديد من المخاوف، والتي من شأنها أن تحول دون التعامل مع هذه البنوك ما لم تواجه هذه المخاوف برقابة قوية، توفر حدا أدنى من الضمانات القانونية(١).

وقد تعاظمت أهمية الرقابة على التزام هذه البنوك بالقوانين السارية في ظل عدم وجود سلطة مركزية على مستوى شبكة الإنترنت تسهر على التزام البنوك بهذه القوانين(٢)، وذلك في ظل تسابق سريع الخطى، وتحد معلن من أجل غزو البيئة الافتراضية من قبل هذه البنوك، من أجل الوصول بالخدمة المصرفية إلى أكبر مستوى من السهولة واليسر، وذلك من خلال التسلح بكل ما هو جديد في عالم الأجهزة والبرامج المعلوماتية، الأمر الذي من شأنه أن يتسبب في حدوث فراغ تشريعي، بسبب عدم ملاءمة القوانين القائمة لهذه المستجدات التي تطرأ

---

(1) **Electronic banking group initiatives and white papers**, Basel committe for banking supervision,Op.Cit,p21;**E-banking**,Federal financial institutions examination council; Op. Cit., p 14.

(2) **Scott F. Uhler, Philippe R. Weiss, Michele M. McGee,** Liability issues and the Internet, Part 1: Electronic Mail, available at: http://www.lib.niu.edu/ipo/1996/ il960266.html

على أسلوب تقديم الخدمة المصرفية الذي تظهر معه وتتجلى أهمية ليس فقط تنظيم قانوني محكم ينظم عمل هذه البنوك، ويحمى المتعاملين معها؛ بل أيضا رقابة مستمرة، تنظر وتحقق في مدى التزام البنك، ومراعاته لهذه القوانين طوال فترة عمله وتشغيله.

ونود قبل التعرض للمعايير الرقابية في هذا الخصوص أن ننوه إلى مسألة بسيطة، وهي أن طبيعة الرقابة على مدى التزام البنك الإلكتروني بالقوانين من عدمه أمر سابق على نشوء منازعات تتعلق بعدم مراعاة هذه القوانين، ومن أجل تجنب نشوئها، وهذا لا يتعارض أبدا مع طبيعة عمل القضاء، والذي يظهر دوره بعد قيام هذه المنازعات، الأمر الذي تظهر معه أهمية هذه الرقابة والتي من شأنها أن تحد من هذه المنازعات وتقلل منها إذا ما طبقت وفق معايير دقيقة ومنضبطة.

١٣٠- وتأتى الرقابة على مدى التزام البنك الإلكتروني بالقوانين والتشريعات التي تحكم وتنظم عمله على شبكة الإنترنت، من خلال التأكد من مراعاة أمور معينة، أهمها(١):

١) النظر في مدى مراعاة البنك للقوانين التي تحكم تعاملاته مع موردى الأجهزة والبرامج اللازمة لتشغيله وعمله، خاصة الجوانب المتعلقة بحماية أصحاب حقوق الملكية الفكرية على هذه الأجهزة والبرامج، وكافة التزامات البنك

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p149; **Is auditing guideline internet banking**; Op. Cit., p. 3; Interagency council issues guidance on electronic financial services and consumer compliance, Federal Financial Institutions Examination Council, 1998,p2, available at: http://www.ffiec.gov/pr071598.htm

الأخرى في مواجهة هؤلاء، ومدى تحمل البنك لمسئولياته القانونية كاملة في هذا المجال، مع الاهتمام بالتعاقدات الجديدة التي يكون البنك قد أجراها للتزود بأجهزة أو برامج يحتاج إليها في عمله.

٢) مدى التزام البنك بالتزاماته مع مزودي الخدمات الإلكترونية المختلفة وفقا للعقود التي تنظم عملهم، خاصة التي يحتاج إليها البنك بصورة مستمرة، مثل عقد الدخول على شبكة الإنترنت، وعقد الإيواء، وذلك للتأكد من مراعاة البنك لحقوق هؤلاء على نحو سليم. أيضا النظر في مدى حرص البنك بصورة مستمرة على التأكد من التراخيص التي تسمح لمزودى هذه الخدمات بتقديم خدماتهم، وإلزامهم بتجديد هذه التراخيص، الأمر الذي يضمن استمرار صلاحيتهم لتقديم هذه الخدمات[١].

٣) النظر في مدى مراعاة البنك للقوانين التي تحكم التعاقدات المصرفية على شبكة الإنترنت، بداية من الإعلان عن هذه الخدمات، مرورا بالأسلوب الخاص بالتعبير عن الإرادة لإبرام العقد، والصيغة التي يظهر عليها، وتحديد واضح للالتزامات، والمسؤوليات المترتبة على الإخلال بهذه الالتزامات، وانتهاءً بتنفيذ هذا العقد بحصول العميل على الخدمة المرجوة، مع مراعاة كافة الضوابط الخاصة بحماية المستهلك والتي ينظمها القانون بخصوص الإعلان والتعاقد عبر شبكة الإنترنت[٢].

---

(1) **Decision of the office of the comptroller of the currency on the application to charter**; Op. Cit, p. 9.

(2) **The new banking delivery system-the internet**, Op, Cit, p. 2; **Decision of the office of the comptroller of the currency on the application to charter**; Op. Cit. p. 9.

٤) التأكد من التزام البنك بالقوانين الخاصة بالحفاظ على سرية بيانات العملاء، ومدى حرصه على إلزام كل العاملين لديه بهذا الأمر، وكذلك مقدمي الخدمات الإلكترونية، وفرض إجراءات رقابية دقيقة على عملهم، بما يجعل كل تحركاتهم تحت سمع وبصر البنك، وتحميلهم مسئوليات مشددة عن الانتهاكات التي تقع منهم في هذا الصدد. ويجب عليه أيضا أن يحيط المتعاملين معه علما بضرورة التقيد بواجبات الحفاظ على السرية، وذلك من خلال قيام البنك بوضع سياسة عامة تحكم التعامل مع موقعه(١)، وترسم الخطوات التي يجب على المتعامل معه اتباعها للحصول على الخدمة المطلوبة، وتحدد له المناطق التي يجوز له التعامل معها، وتلك المحظور عليه الاقتراب منها، ويجب أن يراعى البنك تجديد هذه التعليمات بما يتلاءم مع التطورات التي يشهدها التعامل على شبكة الإنترنت. كما يجب أن يضمن عقود الخدمات المصرفية التزاما بالسرية يقع على عاتق المتعامل معه، ويلحق الإخلال بهذا الالتزام بمسؤولية مشددة في حالة المخالفة(٢).

٥) التأكد من التزام البنك في تعاملاته بمراعاة الضوابط التي نصت عليها

---

(١) هذا وقد صدر في الولايات المتحدة الأمريكية قانون يحمل اسم قانون التحديث المالي (Financial Modernization Act) وذلك في يوليو ٢٠٠١. وقد أولى هذا القانون اهتماما كبيرا بقضايا السرية المتعلقة ببيانات المتعاملين مع المؤسسات المالية، حيث تطلب من هذه المؤسسات ضرورة إخبار هؤلاء المتعاملين بالسياسات الخاصة بالسرية في صورة مكتوبة، كما فرض عليها ضرورة تبنى معايير ملائمة تتعلق بالحفاظ على البيانات الخاصة بالمتعاملين معها، والاستعانة بضوابط أمنية قوية في هذا المجال. انظر

Anita K. Pennathur; Op, Cit, p. 2118; **E-banking,** Federal financial institutions examination council; Op, Cit., p 14.

(2) **William Gram**; Op. Cit., p25.

القوانين الخاصة بالأنشطة الإجرامية، خاصة ما تعلق منها بجـرائم غسيل الأموال (Money laundering)(١)، والتي تفرض على البنك مجموعة من التدابير التي يجب مراعاتها لتجنب استغلال البنك في ارتكـاب مثـل هـذه الجرائم(٢). وهذا ما حرص عليه القـانون الأمريكـي للتجـارة الإلكترونيـة (USA PATRIOT Act Electronic Commerce, 2001) من التـزام البنوك العاملة عبر شبكة الإنترنت بمراعاة قوانين غسيل الأموال، وفـرض رقابة داخلية على معاملاتها للوقاية من حدوث عمليات غسيل الأموال، خاصة أنها تمارس نشاطها عبر حدود الدول، بفضل امتداد شبكة الإنترنـت علـى مستوى العالم بأسره(٣).

---

(١) نظم المشرع المصري قانون مكافحة **غسيل الأموال بالقانون رقم ٨٠ لسنة ٢٠٠٢**، وقد نص على أن:

- ينشأ بالبنك المركزي وحدة مستقلة ذات طابع خاص لمكافحة غسل الأموال وتمثـل فيها الجهات المعنية، وتختص بتلقي الإخطارات الواردة من المؤسسات المالية عـن العمليات التي يشتبه في أنها تتضمن غسيل أموال، وتتولى أعمال التحري والفحـص عما يرد إليها من معلومات (م٣، ٤، ٥).
- تلتزم المؤسسات المالية بإخطار الوحدة عن العمليات المالية التي يشتبه فـي أنهـا تتضمن غسل أموال، وتلتزم أيضا بوضع الـنظم الكفيلـة للتعـرف علـى الهويـة والأوضاع القانونية للعملاء، ولا يجوز لها فتح حسابات أو ربـط ودائـع أو قبـول أموال أو ودائع مجهولة أو بأسماء صورية أو وهمية، كما تلتزم المؤسسات الماليـة بالإمساك بالدفاتر لما تجريه من عمليات مالية، وتحتفظ بهذه السجلات لمدة لا تقـل عن خمس سنوات من تاريخ انتهاء التعامل مع المؤسسة أو من تاريخ قفل الحـساب وأن تضع هذه السجلات تحت تصرف السلطات القضائية والجهات المختصة بتطبيق هذا القانون (المادة ٨، ٩).

(2) **Turner Shawn**; Op.Cit.,p1391; **Is auditing guideline internet banking**; Op. Cit, p. 4.

(3)**The Internet and the Usa patriot Act: Potential implications for**

٦) النظر في مدى تقيد البنك بتعليمات جهة الرقابة الخاصة بالضوابط الأمنية للتعاملات المصرفية على شبكة الإنترنت، والتي تفرض على البنك دائما، ضرورة الاستعانة بأجهزة وبرامج قوية تكفل أمن وسلامة كافة تعاملاته مع عملائه[1]، والنظر في مدى ملاءمة تعاقدات البنك مع الجهات التي تقدم له الخدمات الأمنية، مع طبيعة عمله وقت إجراء الرقابة، وإذا ما كانت هذه التعاقدات كافية لتلبية احتياجات البنك في هذا الخصوص أم أن الأمر يحتاج إلى قيام البنك بتعديل صيغة العقد، وذلك مع الاهتمام بالجوانب الخاصة بالمسؤولية عن الإخلالات التي تحدث في هذا النطاق، وذلك على النحو الذي يوفر ضمانة قوية للمتعاملين مع البنك.

ثالثا: التأكد من استمرار كفاية وجودة المعايير التشغيلية:

١٣١- لاشك في الأهمية القصوى للمعايير التشغيلية في نظام عمل البنك الإلكتروني العامل عبر شبكة الإنترنت، بل لا نكون مبالغين إذا ما ذهبنا للقول بارتباط المعايير السابقة (الأمنية والقانونية) بالنظام التشغيلي للبنك[2]. فمهما

---

electronic privacy- security- Commerce and Government, CRS report for Congress, order code RL31289. available at: epic.org/privacy/terrorism/usapatriot/RL31289.pdf

(1) **Electronic Banking Group Initiatives and White Papers**, Basel committee for banking supervision, Op, Cit, p. 18; **Carlos Martin& Denis Beau**, Les services financiers en ligne, Rapport du groupe de travail, N 5, 15 novembre 2001, p 14

(2) **Risk management principles for electronic banking**, bank for international settlements, p 2, available at: http://www.bis.org/publ/bcbs98.htm; **Elec**

كانت جودة وكفاية الأجهزة والبرامج، ومهما كانت دقــة وبراعــة التنظيمــات القانونية، تبقى المعايير التشغيلية الأساس الذي يبنى عليه كل هذا، وهي المحرك الرئيس لكل هذه العناصر. وتزداد أهمية هذه المعايير في نظام عمل البنك بالنظر إلى الطبيعة المستمرة والمتجددة للمخاطر التشغيلية، فهذه المخاطر لا تبدو عنــد إنشاء البنك فحسب، بل تدور مع البنك أينما دار، وتخيم بظلالها عليه طوال فترة عمله وتشغيله، الأمر الذي يبرز مدى أهمية المعايير التشغيلية في نظــام عمــل البنك(١). يضاف إلى كل ذلك الارتباط المباشر بين المعــايير التــشغيلية للبنــك وسمعته التجارية بين عملائه(٢)، والتي تشغل الحيز الأكبر من اهتمــام البنــك، الأمر الذي زادت أهميته في ظل منافسة قوية بين البنوك وغيرها من المؤسسات المالية الأخرى في بسط الهيمنة والسيطرة على قطاع تقديم الخدمات المالية عبر شبكة الإنترنت(٣)، الأمر الذي يجلى ويبرز أهمية الرقابة على تحصن البنك بهذه المعايير بشكل كاف وفعال، واستمرار هذه الرقابة لضمان التزام البنك بها طوال فترة تشغيله.

١٣٢- ومن أهم المعايير التشغيلية التي يجب أن يلتزم بها البنك، والتي ستكون

---

tronic banking group initiatives and white papers, Basel committee for banking supervision, Op. Cit, p. 15.

(١) د. **طارق طه**، مرجع سابق، ص ٦٦

(2) **Anita K. Pennathur**, Clicks and brick: e-risk management for banks in the age of the internet; Op. Cit, p. 2112.

(٣) وذلك في ظل ظهور اتجاه قوى من قبل بعض الدول يسعى إلى السماح بتقديم بعــض أشكال الخدمات المصرفية (كإصدار النقود لإلكترونية) لمؤسسات مالية غير ائتمانية (كفرنسا). انظر في تفصيل ذلك د. **شريف محمد غنام**، محفظة النقود الإلكترونيــة، مرجع سابق، ص ٨٠

موضـع النظر بالنسبة لجهة الرقابة، ما يلى[١]:

(١) مراجعة أنشطة البنك، والتأكد من توافقها مع عقد تأسيسه، والممارسات المستقرة في هذا الصدد، والنظر في مدى استيعاب هذه الخطط وتلاؤمها مع الواقع العملي لنشاط البنك، وإذا ما كان الأخير قد أدخل عليها تعديلات بسبب التوسيع والتضييق من حجم تعاملاته، أو أبقى عليها منذ وقت تشغيل البنك[٢].

(٢) النظر في أسلوب تعامل إدارة البنك مع العاملين لديه، ومدى قدرتها على التوفيق بين تزويدهم بكافة المعلومات والنصائح والإرشادات اللازمة للتعامل مع أجهزة البنك من أجل تقديم الخدمة المصرفية للعملاء، وبين الرقابة على تعاملهم مع هذه الأجهزة خاصة فيما يتعلق بسرية وخصوصية

---

(1) **Internet banking**; Op. Cit, p. 25; **Is auditing guideline internet banking**; Op. Cit, p. 3.

(٢) هذا وقد نص المشرع المصري في **قانون البنك المركزي والجهاز المصرفي والنقد رقم ٨٨ لسنة ٢٠٠٣** في المادة ٣٨ منه على إلزام البنك بإخطار جهة الرقابة بأي تعديل يجريه في عقد تأسيس البنك، حيث ذهبت هذه المادة إلى أنه: "يجب إخطار البنك المركزي بكل تعديل يراد إجراؤه في عقد تأسيس أي بنك أو في نظامه الأساس، كما يجب الإخطار بكل تعديل في البيانات التي قدمت عند طلب التسجيل".

- وقد عالج **مكتب الرقابة على النقد الأمريكي** (OCC) هذا الأمر، حيث ذهب إلى أن البنك خلال الثلاث سنوات الأول من تشغيله، إذا أراد أن يجرى تغييرا هاما في خطة تشغيله (significant changes to its proposed Operating plan) يجب عليه إخطار مكتب الرقابة على النقد بذلك خلال ثلاثين يوما على الأقل قبل إجراء أي تعديل.

Decision of the office of the comptroller of the currency on the application to charter, Op. Cit., p. 16.

البيانات المخزنة داخل هذه الأجهزة، والخاصة بالمعاملات المصرفية(١).

(٣) النظر في مدى قدرة الجهاز الإدارى للبنك على إدارة علاقة البنك بمقدمي الخدمات الإلكترونية، وعلى وجه الخصوص مدى قدرتهم على إلزامهم بتأدية التزاماتهم القانونية وفقا للعقود التي تحكم وتنظم علاقتهم بالبنك، واتخاذ الإجراءات القانونية اللازمة في حالة تخلف أحدهم عن القيام بالتزاماته.

(٤) النظر في مدى تواصل إدارة البنك مع كافة أجهزة وبرامج البنك، وذلك من خلال القيام باختبارات دورية لنظام عملها، وإجراء الإصلاحات اللازمة إذا ما تطلب الأمر ذلك، والحرص المستمر على القيام بعمليات إحلال لهذه الأجهزة، لإدخال أحدث ما تم التوصل إليه من هذه الأجهزة في نظام عمل البنك(٢).

(٥) تأكد البنك دائما من عمل الأجهزة المسئولة عن أمن الموقع الإلكتروني والشبكة الداخلية للبنك، ومنح هذا الأمر الحيز الأكبر من اهتمام البنك، وذلك من خلال النظر دائما في مدى جودة وكفاية هذه الأجهزة في ضوء نشاط البنك وتعاملاته، الأمر الذي يجعلها ملاءمة لهذا النشاط.

(٦) التأكد دائما من التأهيل الفنى للقائمين على إدارة البنك، وذلك من خلال تطلب جهة الرقابة حضورهم دورات تدريبية بصورة دورية، تحقق

---

(١) د. **طارق طه**، مرجع سابق، ص ٦٧.

(2) **Electronic Banking Group Initiatives and White Papers**, Basel committee for banking supervision, Op. Cit., p. 18; **Interagency council issues guidance on electronic financial services and consumer compliance**; Op. Cit, p. 8.

تواصلهم المستمر مع المتخصصين في هذه المجالات، وذلك على النحو الذي يمكنهم من التناغم مع إيقاع التطورات التي تشهدها الأجهزة الإلكترونية والبرامج الخاصة بها، الأمر الذي يعكس قدرتهم على تشغيل البنك باقتدار.

(٧) النظر في مدى علم ودراية الإدارة بكافة التشريعات القانونية الخاصة بالعمل المصرفي على شبكة الإنترنت، والتعليمات والتوجيهات الصادرة عن جهة الرقابة، ومدى الالتزام بها وتفعيلها على مجمل نشاط البنك وتعاملاته، الأمر الذي تظهره العقود المصرفية التي يقوم البنك بإبرامها مع العملاء، وأسلوب تعامل البنك مع العاملين لديه، ومزودي الخدمات الإلكترونية.

١٣٣- وبعد استعراض أهم المعايير التي توجه إليها جهود جهة الرقابة طوال فترة عمل وتشغيل البنك، والتي استجمعت معظم نقاط الضعف في نظام عمل البنك، والت تعكس الأهمية القصوى للرقابة في حياة هذه البنوك، وتؤكد دورها المحوري كضمانة للبنك، والمتعاملين معه، ومن ثم حركة التجارة الإلكترونية على شبكة الإنترنت في مجموعها. لكن كل هذا لا يمنعنا من القول بضرورة تقيد جهة الرقابة عند ممارسة دورها الرقابي على البنك الإلكتروني العامل عبر شبكة الإنترنت بأمور معينة، تعكس أيضا الحرص على التعظيم من ضمانات البنك وعملائه. ومن أهم هذه الأمور:

(١) ضرورة الاستعانة بمراقبين مؤهلين لممارسة الرقابة بما يتناسب مع طبيعة عمل البنك على شبكة الإنترنت، وذلك حتى يتسنى لهم التأكد من استيفاء البنك

للمتطلبات الرقابية والكشف عن أي عوار في نظام عمله(١).

٢) مراعاة الطبيعة الخاصة للبنك، والتذكر دائما أنه تاجر يسعى إلى تحقيق الربح في المقام الأول، الأمر الذي يفرض على جهة الرقابة ألا تغالي في الإجراءات والأعباء الرقابية، وذلك على النحو الذي يقيد من حرية الحركة بالنسبة لممارسة البنك لنشاطه، بل إن هذا الأمر تزداد أهميته أكثر في نظام عمل البنك العامل عبر شبكة الإنترنت، الذي أخذ على عاتقه تحمل العناء الناتج عن التعامل في البيئة الافتراضية، سواء على صعيد التجهيزات الفنية والتشغيلية اللازمة لذلك وما يحتاجه ذلك من الاستعانة بالفنيين المتخصصين، أم على صعيد المخاطر الأمنية التي تحيطه من كل مكان، فقد تحمل كل هذا العناء سعيا لمزيد من السهولة في التواصل مع العملاء، ومن ثم زيادة الربح، ومن ثم يجب ألا تكون الرقابة قيدا يعوقه عن تحقيق ذلك، بل يجب على جهة الرقابة أن تحقق نوعا من التوازن بين المصالح المتعارضة في هذا الخصوص، وذلك من خلال فرض إجراءات رقابية دقيقة وقوية، ولا تثقل كاهل البنك في ذات الوقت بأعباء كثيرة.

٣) حرص جهة الرقابة دائما على عدم الاقتراب من المناطق التي تخزن بها البيانات الخاصة بالمعاملات المصرفية، والتي يجب أن تنظر إليها دائما على أنها حصون منيعة، تحيا في كنف السرية، وتحت ظل الخصوصية(٢)، وذلك

---

(1) **Is auditing guideline internet banking**; Op. Cit, p. 4.

(٢) وقد راعى المشرع المصري هذا الأمر في قانون البنك المركزي والجهاز المصرفي والنقد سالف الذكر، حيث نص في المادة (٩٧) على أن: "تكون جميع حسابات العملاء وودائعهم وأماناتهم وخزائنهم في البنوك سرية، ولا يجوز الإطلاع عليها أو إعطاء بيانات عنها بطريق مباشر أو غير مباشر إلا بإذن كتابي من صاحب الحساب أو

على النحو الذي يجعل جهة الرقابة حريصة دائما على ألا تفرض إجراءات من شأنها الكشف عن هذه البيانات أو الاطلاع عليها، إلا في حالات الضرورة، على أن تقدر الضرورة بقدرها. فسرية البيانات المصرفية أمر لا يتعلق بسمعة البنك وحسب، بل هو وثيق الصلة أيضا بمصلحة العملاء، الأمر الذي يجب معه أن تحرص جهة الرقابة دائما على أن تعزز من سرية وخصوصية هذه البيانات، وذلك من خلال فرض إجراءات من شأنها أن تنظر في مدى مراعاة البنك لهذا الأمر.

وقد شهد هذا الأمر أهمية خاصة في حياة البنك الإلكتروني العامل عبر شبكة الإنترنت، حيث إن السرية والخصوصية لم تعد مقصورة على حسابات العملاء وودائعهم لدى البنك فحسب، بل يمتد الأمر أيضا ليشمل قاعدة البيانات الخاصة بالبنك، والتي تحتوى على البيانات الخاصة بالعملاء وتعاملاتهم مع البنك، ككلمات السر الخاصة بالدخول على الموقع الإلكتروني للبنك أو دخول العميل على حسابه والتعامل عليه، أيضا البيانات الخاصة بالتشفير وما يرتبط به

الوديعة أو الأمانة أو الخزينة أو من أحد ورثته، أو من أحد الموصى لهم بكل أو بعض هذه الأموال أو من النائب القانوني أو الوكيل المفوض في ذلك أو بناء على حكم قضائي أو حكم محكمين. ويسرى هذا الحظر على جميع الأشخاص والجهات التي يخولها القانون سلطة الإطلاع أو الحصول على الأوراق أو البيانات المحظور إفشاء سريتها طبقا لأحكام هذا القانون، ويظل هذا الحظر قائما حتى لو انتهت العلاقة بين العميل والبنك لأي سبب من الأسباب".

- كما نص في المادة (٩٨) من ذات القانون على الآتي: "للنائب العام أو لمن يفوضه من المحامين العامين الأول على الأقل من تلقاء نفسه أو بناء على طلب جهة رسمية أو أحد من ذوى الشأن، أن يطلب من محكمة استئناف القاهرة الأمر بالإطلاع أو الحصول على أية بيانات أو معلومات تتعلق بالحسابات أو الودائع أو الأمانات أو الخزائن المنصوص عليها في المادة السابقة أو المعاملات المتعلقة بها إذا اقتضى ذلك كشف الحقيقة في جناية أو جنحة قامت الدلائل الجدية على وقوعها".

من بيانات خاصة بمفاتيح التشفير، والتوقيع الإلكتروني، فالبنك الإلكتروني العامل عبر شبكة الإنترنت ما هو إلا تدفق هائل من البيانات عبر مجموعة من الأجهزة والشبكات، الأمر الذي يعظم من سرية وخصوصية هذه البيانات حتى في مواجهة جهة الرقابة.

٤) مراعاة جهة الرقابة للبعد التنافسي الذي أصبح من أكبر التحديات التي تشغل بال البنك الإلكتروني العامل عبر شبكة الإنترنت(١)، فساحة المنافسة فقدت هويتها الوطنية، واتسعت لتشمل العالم بأسره، وذلك تأثرا بالطابع الدولي لشبكة الإنترنت، الأمر الذي قد يترتب عليه وجود فوارق بينية في المعاملات الرقابية من قبل دولة عن أخرى(٢)، بما ينعكس سلبا على البنوك التي تخضع

---

(1) **Jennifer Iser**; Op, Cit, p1; **Tahir Masood Qureshi, Op. Cit, p.** 5.

2 / وقد ظهر هذا الأمر جليا بخصوص أحد الشركات التي تقدم خدمات الدفع الإلكتروني عبر شبكة الانترنت (Paypal) حيث اعتبرت المملكة المتحدة هذه الشركة بنك في ضوء ما تكتفي به قوانينها من أن البنك هو المؤسسة التي تقوم بتلقي الودائع من الأفراد وتقوم بإعادة إقراضها، في حين لم تعتبرها الولايات المتحدة بنكا، حيث إنها لا تخضع عند إنشائها للمتطلبات الرقابية الخاصة بالبنوك.

Andrés Guadamuz Gonzalez, E-commerce – payment systems (PayPal: the legal status of C2C payment systems), Computer law & security report Vol. 20 no. 4, 2004, P. 296.

- و قد أكد على هذا المعنى التقرير الصادر عن البنك المركزي الهندي ٢٠٠١، والذي أشار إلى اتساع ساحة السباق والمنافسة في عمل البنوك العاملة عبر شبكة الانترنت، في ظل اختلاف المعايير الرقابية المتبعة من قبل كل دولة، في ظل غياب سلطة مركزية تصيغ معايير موحدة تلزم الكافة. راجع العنوان الإلكتروني التالي:

www.rbi.org.in/Scripts/PublicationReportDetails.aspx

لإجراءات رقابية مشددة في بلادها، الأمر الذي يجب معه على جهة الرقابة أن تضع إجراءات رقابية تحقق الهدف المنشود، وتراعى في ذات الوقت المنافسة وتحديداتها في حياة البنك العامل عبر شبكة الإنترنت، وما يستتبع ذلك من وجود إجراءات رقابية تفطن لذلك، وتسعى إلى تمكين البنك من الاستفادة من التكنولوجيا ومعطياتها المتجددة، بل والأخذ بيده في هذه البيئة الجديدة، التي قد يحتاج فيها للنصح والإرشاد والتوجيه من أجل القدرة على التعامل مع تحديداتها المختلفة.

١٣٤- وإذا كان ما سبق التعرض له من ضوابط رقابية بمرحلتيها (الحصول على ترخيص لإنشاء البنك على شبكة الإنترنت، والإجراءات الرقابية على عمله)، هي مجرد تنظيمات رقابية فردية تباشرها كل دولة في مواجهة البنوك التي تنشأ وفقا لقوانينها، إلا أن هناك بعدا يظل غائبا عن هذه التنظيمات، على الرغم مما له من أهمية بالغة في نظام عمل هذه البنوك، ورغم ما يصاحبه من مخاطر جمة، وهو البعد الدولي لنشاط هذه البنوك، والمستمد من دولية البيئة التي تعمل فيها، وهى شبكة الإنترنت، بما يحتاج معه الأمر إلى إجراءات جماعية للتصدي له، الأمر الذي يدفعنا للتساؤل عن طبيعة التنظيمات الدولية في مجال الرقابة على البنوك العاملة عبر شبكة الإنترنت؟

وقد تصدت مجموعة البنك الإلكتروني (Electronic Banking Group) في لجنة بازل للرقابة على البنوك للرد على هذا التساؤل، حيث ذهبت هذه اللجنة إلى ضرورة وجود نوع من التواصل بين جهات الرقابة المختلفة فيما يتعلق بأنشطة البنوك العاملة عبر شبكة الإنترنت، مثل هذا التواصل سيكون بمثابة الخطوة الأولى على طريق إيجاد منهج موحد ومنسق فيما بين هذه الجهات

بخصوص هذا الأمر.

وقد بررت هذه اللجنة الاكتفاء بمجرد التواصل في هذه المرحلة بالقول بأن الأنشطة المصرفية الإلكترونية لا تزال في مراحلها الأولى (Early stages)، ومن غير المناسب وضع معايير صارمة (Normative standards) ربما تعوق الابتكار التكنولوجي والاستفادة منه في العمل المصرفي. وطبقا لأسلوب عمل هذه المجموعة في هذه المرحلة، فإنها سوف تركز على تسهيل عمليات الحوار والتحليل بين فيما بين جهات الرقابة، والتي يمكن أن تؤدى في النهاية إلى وضع إطار رقابي دقيق للأنشطة المصرفية الإلكترونية على الصعيد الدولي. وفى هذا الخصوص فقد حددت مجموعة البنك الإلكتروني مجموعة من المعايير[١]، يجب أن ينصب عليها الحوار والتواصل بين جهات الرقابة في هذه المرحلة، وهى[٢]:

---

(١) وتعد هذه المعايير شكلاً من أشكال التعاون الدولي في مجال الرقابة على البنوك الإلكترونية العاملة عبر شبكة الانترنت، والتي تأخذ الطابع الإيصائى (Recommended mode) في مواجهة جهات الرقابة، ولا تلتزم هذه الجهات بهذه المعايير، حيث تهدف لجنة بازل من ورائها إلى وضع نموذج للمعايير الرقابية تتأسى بها الجهات الرقابية في التعامل مع البنوك العاملة عبر شبكة الانترنت. وقد أنشئت لجنة بازل في عام ١٩٧٥، وهى عبارة عن منتدى يضم رؤساء البنوك المركزية، والسلطات الرقابية على مستوى العالم.

Apostolos Ath. Gkoutzinis; Op. Cit., p. 150.

(2) **Electronic banking group initiatives and white papers**, Op. Cit, p.1.

١)- التعاون لرصد كل أشكال المخاطر التي تواجهها البنوك بالفعل أثناء تقديمها للخدمات المصرفية عبر شبكة الإنترنت لإعداد دليل يحصر ويحدد هذه المخاطر.

والهدف من وراء صياغة هذا الدليل هو حصر كافة أشكال المخاطر التي يمكن أن تتعرض لها البنوك على شبكة الإنترنت. وذلك من أجل فهم جيد ومتعمق لطبيعة هذه المخاطر ومصادرها، ومن ثم صياغة مقترحات رقابية ملاءمة لمواجهة هذه المخاطر، وذلك على النحو التالي:

أ- التعاون فيما بين جهات الرقابة لتحديد كافة أنواع المخاطر الأمنية، وأشكالها المختلفة، ومصادرها، خاصة التي يقف وراء وجودها هيمنة التكنولوجيا على مجريات العمل المصرفي، من أجهزة وبرامج وشبكات.

ب- دراسة النتائج المحتملة للتطبيقات التكنولوجية الجديدة في نظام عمل البنوك، ومدى قابلية هذه التطبيقات للعمل على نماذج العمليات المصرفية المعروفة، وأشكال الخدمات المصرفية الجديدة التي يمكن أن تتسبب في وجودها هذه التكنولوجيا (خاصة خدمات المعلومات)، وما إذا كان هذا الأسلوب في ممارسة العمل المصرفي مصحوبا بمخاطر جديدة لم تكن معروفة من قبل، وتحديد مصادر هذه المخاطر، ومدى تأثيرًاها على تقديم الخدمات المصرفية خاصة على صعيد المعاملات الدولية، والمقترحات بشأن التصدي لها، وذلك كله من واقع الممارسة العملية.

٢)- التعاون فيما بين الجهات الرقابية لتسهيل عمليات الرقابة على النشاط الدولى للبنوك الإلكترونية:

وتهدف مجموعة البنوك الإلكترونية من هذا إيجاد نوع من التواصل بين جهات الرقابة في حالة مباشرة البنك لنشاطه عبر الحدود (cross-border e-banking activities)، وذلك للتثبت من استيفائه للمعايير الرقابية طبقا لقوانين الدولة التي نشأ في ظلها، ومدى كفاية هذه المعايير في ضوء القوانين الخاصة بالدولة التي يتم ممارسة النشاط المصرفي في مواجهة المقيمين على أرضها. في محاولة للتوصل إلى صيغة شبه موحدة لهذه المعايير من واقع الممارسة العملية

٣)- تنشيط جهود التعاون بين جهات الرقابة على البنك الإلكتروني وكافة مؤسسات القطاع العام والخاص:

وسوف تظهر جهود التعاون في هذا الصدد من نواحي متعددة كالتالي:

أ- يجب على جهات الرقابة أن تتبادل المعلومات بصورة مستمرة مع المؤسسات الإقليمية التي تتعامل معها البنك الإلكتروني، وذلك لاستطلاع آرائها حول طبيعة المخاطر التي تواجهها هذه البنوك أثناء تعاملها مع هذه الجهات، والممارسات العملية من قبل هذه البنوك لمواجهة هذه المخاطر.

ب- يجب على جهات الرقابة أن تعمل على تبادل المعلومات والبيانات بينها وبين الشركات القائمة على تقديم الخدمات الإلكترونية للبنوك على شبكة الإنترنت، ووجوب تقييم هذه المعلومات في ضوء نشاط هذه البنوك، وذلك للنظر في مدى تأثيرًا وجود هذه الشركات في حياة هذه البنوك، والمخاطر المرتبطة بذلك وسبل مواجهتها.

ج- يجب على جهات الرقابة أن تمد جسور التعاون بينها وبين جهات الرقابة على الأسواق المالية الدولية (International Financial Market) مثل الاتحاد الدولى للرقابة على أعمال التأمين (International Association of Insurance Supervisors)، ولجنة المدفوعات ونظم التسوية (Committee on Payment and Settlement Systems) وذلك لتبادل المعلومات المتعلقة بمخاطر التجارة الإلكترونية، والشائعة في نظام عمل البنك الإلكتروني، والتي من أهمها قضايا مخاطر التشغيل، والمخاطر القانونية، والمخاطر الأمنية، لتطوير المعايير الرقابية المرتبطة بهذه القضايا.

٤)- يجب على جهات الرقابة أن تشجع وتسهل تبادل برامج التدريب على المراقبين على البنك الإلكتروني وكافة المواد اللازمة لتطوير عملهم:

بالنظر إلى ما تتسم به التكنولوجيا من تعقيد وسرعة من ناحية، وما تشهده من تطورات سريعة في مجال العمل المصرفي على شبكة الإنترنت من ناحية أخرى، فإن المراقبين على هذه البنوك يواجههم تحد كبير فيما يتعلق بالخبرة الكافية للتعامل مع هذه الأمور، وما تطرحه من مستجدات، الأمر الذي ستظهر معه الحاجة إلى ضرورة تبادل البرامج التدريبية والوسائل التعليمية في هذا المجال بين المراقبين على مستوى العالم بأسره. ولاشك في الأهمية البالغة لهذا الأمر، حيث يخلق نوعا من تبادل الخبرات في هذا المجال، ومن ثم تعظيم حجم الإستفادة، الأمر الذي ينعكس على جودة وكفاية المعايير الرقابية، وذلك من خلال تحقق الأهداف المبتغاة من الرقابة على نشاط البنوك، ومراعاة عدم وضع عراقيل في وجه البنك للاستفادة من التكنولوجيا ومعطياتها.

هذا وقد صدر عن لجنة بازل في يوليو ٢٠٠٣ دليل رقابي نموذجي[١] يتضمن مجموعة من الضوابط تحمل ذات المعاني والأهداف الموجودة في المعايير السابقة[٢].

١٠٠- ولاشك في الأهمية البالغة لتلك الخطوة التي قامت بها لجنة البنك الإلكتروني التابعة للجنة بازل للرقابة على البنوك في هذه المرحلة، حيث تظهر الحاجة إلى فهم جيد لطبيعة وحجم المخاطر المحيطة بالبنوك العاملة عبر شبكة الإنترنت الذي ييسر صياغة قواعد رقابية تحمل صيغة شبه موحدة فيما بين الجهات الرقابية الذي يساعد بلا شك على نجاح هذه البنوك في تأدية عملها، وتخطى العقبات المتعلقة بممارسة النشاط المصرفي عبر الحدود، لكنها لا تزال في حاجة إلى خطوة ثانية على ذات الطريق، خطوة تتعلق بوجود معايير رقابية موحدة تحمل الطابع الملزم، وذلك من خلال صياغة اتفاقية دولية في مجال العمل الرقابي على نشاط هذه البنوك، وذلك لضمان وجود حد أدنى من الشروط والمعايير، يجب أن تتوافر في البنك عند إنشائه، وأثناء مباشرته للعمل المصرفي في مواجهة المقيمين في كل دول العالم. والقول بالطابع الملزم في هذه المرحلة له ما يبرره، فالبيئة المفتوحة التي تحيى فيها هذه البنوك، والتي يغيب عنها السلطة المركزية المهيمنة على مجرى التعامل عليها، أمور من شأنها أن تثير القلق حول مشروعية البنوك العاملة في هذه البيئة، ومشروعية ما تقدمه من خدمات، ومدى استيفائها للضوابط الأمنية والقانونية والتشغيلية المؤهلة لمباشرتها لنشاطها، كل ذلك كان الدافع وراء القول بالطابع الموحد والملزم للمعايير الرقابية

---

(١) هذا الدليل متاح على العنوان الإلكتروني التالي:
http://www.bis.org/pub1 bcbs98.htm

(2) **Apostolos Ath. Gkoutzinis**; Op. Cit, p. 153.

التي تحكم إنشاء وعمل هذه البنوك.

الباب الثاني

التعاقدات المصرفية للبنك الإلكتروني على شبكة الإنترنت

١٣٥- تعد الخدمات المصرفية هي محور نشاط أي بنك (إيداع، سحب، تحويل. ..)، وتعد العقود المصرفية هي الوسيلة التي يمكن له من خلالها التعامل مع عملائه بخصوص هذه الخدمات، حيث تتولى هذه العقود مهمة تنظيم علاقة البنك وعميله من خلال تحديد التزامات ومسؤوليات الأطراف بخصوص الخدمة المصرفية محل العقد.

١٣٦- ويجرى العمل في ظل نظام البنوك التقليدية على إبرام العقد المصرفي من خلال ذهاب العميل إلى مقر البنك وقيامه بطلب خدمة مصرفية معينة، والتعاقد عليها في مقر البنك. وقد كانت القواعد القانونية الحاكمة لهذه العقود سواء فيما يتعلق بمضمونها أم بطريقة إبرامها تقوم على أساس أنها تعاقدات مباشرة تتم في ظل حضور مادي للمتعاقدين، بما يسمح للبنك بأن يتعرف على شخصية العميل ويتأكد من ضماناته المالية المؤهلة لحصوله على الخدمات التي يقدمها، بحيث إذا أطمأن البنك إليه، يطلعه على شروط تقديم هذه الخدمة، فإذا وافق العميل عليها قام بتوقيع العقد، وقام البنك بتنفيذ الخدمة له. لكن مع التطور الذي شهده العمل المصرفي في ظل فكرة البنك الإلكتروني على شبكة الإنترنت، والذي تمثل في غياب التواجد المادي للبنك في البيئة الواقعية، وظهوره في صورة افتراضية على شبكة إلكترونية للاتصال عن بعد، تتيح التواصل بين الأطراف المتعاقدة في ظل غياب مادي لهما بالمعنى المألوف في عمل البنوك

التقليدية.

هذا التطور طرح بدوره العديد من التساؤلات القانونية، كان في مقدمتها: هل صاحب التطور الذي شهده أسلوب تقديم الخدمة المصرفية في نظام البنك الإلكتروني على شبكة الإنترنت تغير في القواعد القانونية التي تحكم وتنظم العقود المصرفية، سواء من ناحية إبرامها أم من ناحية مضمونها؟ بمعنى أخر هل استطاعت القواعد القانونية التي تنظم التعاقد المصرفي التقليدي أن تستوعب المتغيرات التي طرأت على أسلوب تقديم الخدمات المصرفية على شبكة الإنترنت، أم أن تقديم هذه الخدمات بهذه الوسيلة أحدث فراغا تشريعيا باتت معه الحاجة ملحة إلى صياغة قواعد قانونية جديدة قادرة على التكييف مع هذه المتغيرات وتلبية احتياجاتها؟ هذا من ناحية.

ومن ناحية أخرى: هل تقديم البنك لخدماته عبر شبكة الإنترنت ساعده على استحداث خدمات مصرفية جديدة، ما هو التنظيم القانوني المقترح لهذه الخدمات؟

ومن أجل الوقوف على إجابة كافية وشافية لهذه التساؤلات وغيرها، فإن الأمر يحتاج إلى تفصيل لماهية العقود المصرفية على شبكة الإنترنت؛ من خلال تعريف هذه العقود وبيان أهم خصائصها، وذلك للوقوف على طبيعة التغيرات والاختلافات التي طرأت على هذه العقود، ثم التعرف على القواعد التي تحكم وتنظم إبرامها (فصل أول). على أن يلي ذلك عرض لأهم نماذج للخدمات المصرفية المستحدثة في نظام البنك الإلكتروني على شبكة الإنترنت (فصل ثاني)، وذلك على التفصيل التالي:

الفصل الأول

ماهية العقود المصرفية على شبكة الإنترنت وقواعد إبرامها

١٣٧- بداية تجدر الإشارة إلى الدور البالغ الأهمية الذي تلعبه العقود المصرفية على شبكة الإنترنت في خدمة المعاملات التجارية بصورة عامة. ويقف وراء هذا الدور طبيعة الخدمات محل هذه العقود، والتي تتمثل معظمها في خدمات الدفع الإلكتروني (إصدار النقود الإلكترونية، التحويل الإلكتروني للنقود، تحصيل الشيكات المعالجة إلكترونيًا، التعامل ببطاقات الائتمان بأنواعها المختلفة. .....). والتي تعد مرحلة لا غنى عنها في أية معاملة تجارية (تقليدية أو إلكترونية) لتسوية المدفوعات الناشئة عن هذه المعاملة[1]. فكما يرى البعض- وبحق- البنك الإلكتروني من خلال تعاقداته المصرفية يكاد يهيمن على نظم الدفع الإلكتروني التي تتم على شبكة الإنترنت[2].

وتعد العقود المصرفية على شبكة الإنترنت من قبيل العقود الإلكترونية التي تبرم عن بعد، حيث إنها تبرم باستخدام وسيلة إلكترونية للاتصال عن بعد، وبدون حضور مادي للمتعاقدين بالمعنى التقليدي.

والملاحظ على الرغم من أهمية هذه العقود، إلا أن معظم التشريعات العربية بصورة عامة قد غفلت عن وضع تنظيم قانوني للعقود المصرفية على شبكة الإنترنت، تحدد من خلاله ماهيتها، والقواعد التي تحكم إبرامها، وذلك على

(1) **James E Backhouse**; Op. Cit, p. 30.

(2) **Apostolos Ath. Gkoutzinis**; Op. Cit, p. 7.

الرغم من أهمية هذا في ظل ما ينفرد به التعاقد المصرفي من خصائص تميزه، وتلائم العمل المصرفي، الأمر الذي ألقى بعبء هذه المسؤولية على عاتق الباحثين القانونيين لمحاولة تدارك هذا الأمر.

ويمكن القول إن تحديد ماهية العقود المصرفية على شبكة الإنترنت قد أثار على وجه الخصوص العديد من الإشكالات القانونية، ويعود ذلك إلى ما تتمتع به هذه العقود من خصائص معينة تميزها عن غيرها من العقود الإلكترونية الأخرى. هذا من ناحية، ومن ناحية أخرى تعدد وتنوع العمليات التي يمكن للبنك أن يقدمها عبر شبكة الإنترنت، يضاف إلى ذلك، أن هذه العقود تنظم مسائل فنية خاصة تحتاج إلى قواعد مفصلة لتنظمها، حيث لا يكفى معها القواعد العامة أو المجملة.

لذلك سنقسم هذا الفصل إلى مبحثين، نخصص المبحث الأول فيه لبيان ماهية العقود المصرفية على شبكة الإنترنت، أما المبحث الثاني فنتناول فيه قواعد إبرام هذه العقود، وذلك على التفصيل التالي:

المبحث الأول

ماهية العقود المصرفية على شبكة الإنترنت

١٣٨- في سبيل تحديد ماهية العقود المصرفية على شبكة الإنترنت، فأن الأمـر يتطلب الوقوف على تعريف واضح لهذه العقـود (مطلـب أول)، وبيـان أهـم خصائصها (مطلب ثانى).

المطلب الأول

تعريف العقود المصرفية على شبكة الإنترنت

١٣٩- يشكل وضع تعريف محدد للعقود المصرفية على شبكة الإنترنت أهميـة خاصة، تتجلى بالنظر إلى حداثة هذه العقود، وما يترتب على ذلك من رغبة في معرفة وجه الحداثة وآثارها. هذا من ناحية، ومن ناحية أخرى فقد لعبت شـبكة الإنترنت دورا كبيرا في تسهيل التعامل التجاري عبر العالم بأسره، ممـا دفـع بالعديد من الشركات والمؤسسات إلى تقديم بعض الخدمات الماليـة عبـر هـذه الشبكة كتلك التي يقدمها البنك، الأمر الذي تسبب في حدوث لبس وخلط دعـت معه الحاجة إلى الوقوف على تعريف محدد للعقـود المـصرفية علـى شـبكة الإنترنت لفض هذا التشابك، وأخيرا العقود المصرفية على شبكة الإنترنت ــ كما سبق أن ذكرنا ــ تعد من قبيل العقود الالكترونية؛ تلك التي تشهد تعددًا وتنوعًـا

كبيرًا، مما يدعو إلى توضيح وتمييز العقود المصرفية من بينها، وذلك بتعريفها.

وتأتي هذه الأهمية في ظل خلو النظام القانوني المصري من نص يعرف العقود المصرفية على شبكة الإنترنت، كما لم يظهر لنا نظام قانوني آخر وضع تعريفا لهذه العقود، الأمر الذي يتطلب تأصيل تعريف مناسب في ضوء طبيعة الخدمات المصرفية (باعتبارها محلا لهذه العقود)، وفى ضوء طبيعة الوسيلة الإلكترونية المستخدمة في التعاقد (شبكة الإنترنت).

وقبل أن نتعرض لتعريف العقود المصرفية على شبكة الإنترنت يبدو لنا أن هناك خطوة سابقة على ذلك، من شأنها أن تجلى لنا الرؤية أكثر حول مفهوم هذه العقود، وتبرز لنا وجه خصوصيتها، هذه الخطوة هي تحديد أطراف هذه العقود، وذلك على النحو التالي:

١- البنك الإلكترونى كأحد أطراف العقد المصرفى على شبكة الانترنت:

١٤٠- قد يبدو للوهلة الأولى إن القول بوجود البنك الإلكتروني كأحد أطراف العقد المصرفي على شبكة الإنترنت أمر مفترض، وذلك بالنظر إلى طبيعة العمليات المصرفية التي لا يحترف القيام بها إلا البنوك. لكن عند إرجاع النظر فيما شهدته المعاملات المالية من تطور كبير خاصة بعد التزاوج الذي تم بينها وبين وسائل الاتصال الحديثة- خاصة شبكة الإنترنت- يلاحظ أن هذا التزاوج قد أسفر عن ميلاد مؤسسات غير ائتمانية تقوم بتقديم بعض الخدمات التي هي في الأصل خدمات مصرفية(1)، والتي كانت بالأمس القريب حكرا على البنوك

(1) **Valters Kaze, Ilona, Erika Sumilo, Roberts Skapars**, Trends and priorities in the development of the Latvian banking services in the context of emerging knowledge based economy: case of E-

وحدها[1]. فمثلا في مجال إصدار النقود الإلكترونية نجد أن هناك العديد من الشركات تنافس البنوك في هذا الأمر. وقد راعت التشريعات التي اعترفت بهذه النقود كوسيلة للدفع، تنظيم نشاط هذه الشركات (بعد الحصول على ترخيص بذلك) من خلال عقود تبرمها مع من يريد التعامل بهذه النقود.

ومن هذه التشريعات ما صدر عن البرلمان الأوربي (EP) من توجيهات في ١٨/٩/٢٠٠٠، رقمي (٢٠٠٠/٤٦ - ٢٠٠٠/١٢)، وذلك بعد سلسلة من التوضيات والمقترحات، والتي نادت بالسماح للمؤسسات غير الائتمانية بإصدار النقود الإلكترونية[2]، الأمر الذي يدفعنا إلى أن نوضح ونبرز أمرًا هام، وهو أن العقود المصرفية التي سنتناولها في هذا البحث سواء بالتعريف، أو بشرح أحكامها هي العقود التي يكون أحد أطرافها دائما البنك الإلكتروني العامل عبر شبكة الإنترنت.

Banking, University of lativia, 2007, p. 176; **Report on electronic money**; Op. Cit, p. 8.

(١) ولا يزال هذا الاحتكار قائما في بعض الدول كمصر التي يقتصر إصدار النقود الإلكترونية على البنوك فقط. وهذا ما يتضح من صياغة الضوابط الرقابية الخاصة بالعمليات المصرفية الإلكترونية، والتي أصدرها البنك المركزي المصري في ٢٠٠٢/٢/٢٨، حيث قصر إمكانية إصدار هذه النقود على البنوك وحدها (بعد الحصول على ترخيص من البنك المركزي بذلك) دون غيرها من المؤسسات الائتمانية أو غير الائتمانية.

انظر: **الضوابط الرقابية للعمليات المصرفية الإلكترونية وإصدار وسائل دفع للنقود الإلكترونية**، البنك المركزي المصري، الجلسة المنعقدة بتاريخ ٢٨ فبراير ٢٠٠٢، ص٤، متاح على العنوان الإلكتروني التالي:

http://www.cbe.org.eg/public/Regulations%20of%20The%20Electronic%20Banking%20Operations.doc

(٢) د. شريف محمد غنام، محفظة النقود الإلكترونية، مرجع سابق، ص٨٢، وما بعدها.

٢- المقصود بالعميل كأحد أطراف العقد المصرفى على الانترنت:

١٤١- تبدو أهمية تحديد المقصود بعميل البنك الإلكتروني بمناسبة تعريف العقود المصرفية على شبكة الإنترنت، في معرفة المواصفات التي يجب أن تتوافر في الطرف المناظر للبنك الإلكتروني في العقد المصرفي، والذى يتمتع بمركز قانوني خاص، يحتاج على أثره لمعاملة قانونية خاصة باعتباره الطرف الضعيف في مواجهة البنك، كما يفرض عليه هذا المركز بعض الالتزامات القانونية الخاصة.

ويمكن القول بأنه لا يوجد نص فى القانون المصرى يضع تعريفا لعميل البنك الالكترونى، ولا حتى تعريف لعميل البنوك بصورة عامة. ولم يظهر لنا سوى نصوص متفرقة عرفت العميل فى مناسبات خاصة.

فقد عرفه قانون التجارة الجديد ١٧ لسنة ١٩٩٩ فى المادة (٦/٥١٦) بخصوص تطبيق أحكام الشيك المسطر بأنه " كل شخص له حساب لدى المسحوب عليه وحصل منه على دفتر شيكات أو كان من حقه الحصول على هذا الدفتر".

والملاحظ على هذا التعريف أنه لا يعد حجة فى خصوص تعريف عميل البنك؛ حيث أتسم بنظرة ضيقة، ظهرت فى قصره تعريف العميل فقط فى خصوص أحكام الشيك المسطر، وليس تعريف عميل البنك بصورة عامة.

عرف العميل أيضا فى قرار رئيس مجلس الوزراء رقم ٩٥١ لسنة ٢٠٠٢ بإصدار اللائحة التنفيذية لقانون مكافحة غسل الأموال الصادر بالقانون رقم ٨٠

لسنة ٢٠٠٣[١]، حيث ذهب بأنه " الشخص الطبيعي أو الاعتبارى الذي تفتح المؤسسة المالية حسابا باسمه، أو تنفذ عملية لحسابه، أو تقدم له خدمة".

ويلاحظ على هذا التعريف أمران:

الأول: أن هذا التعريف أوضح المقصود بعميل كافة المؤسسات المالية، وليس البنوك فقط.

الثاني: أن هذا التعريف يبين المقصود بالعميل في خصوص قانون مكافحة غسل الأموال، وليس تعريف العميل في خصوص الحصول على الخدمات المصرفية الالكترونية بصورة عامة.

والوضع على هذا النحو يعكس فراغا تشريعيا في النظام القانوني المصري بخصوص تحديد المقصود بعميل البنك الإلكتروني.

وفى ظل هذا الصمت التشريعى، ذهب جانب من الفقه[٢] يعرف عميل البنك بأنه عن أي شخص طبيعى أو معنوي يحصل على إحدى الخدمات المصرفية التي يقدمها البنك، بموجب عقد يلتزم الأخير بموجبه بتقديم هذه الخدمة، كما يلتزم العميل بدفع مقابل لهذه الخدمة.

ويبدو أن هذا التعريف لم يثر خلافا بين الفقه، حيث أتسمت عباراته بالعمومية على النحو الذى عالج من خلاله ضيق الألفاظ التى جاءت فى التعريفات السابقة.

لكن التساؤل الذي أثار اختلافا تعلق بمدى إشتراط أن يكون للشخص حساب

---

(١) انظر الجريدة الرسمية، العدد ٢٠ مكرر، ٢٢ مايو، ٢٠٠٢، المادة (١)

(2) **William Gram**; Op. Cit, p. 27.

لدى البنك حتى يحظى بوصف العميل، أم يكفى مجرد حصوله على أحد الخدمات المصرفية التي يقدمها البنك ليحظى بهذا الوصف حتى ولو لم يكن لديه حساب لدى البنك؟

ذهبت المحاكم الإنجليزية في أحد أحكامها لتعريف المقصود بعميل البنك بأنه الشخص الذي يوجد لديه حساب لدى البنك(١).

على صعيد آخر تبنى جانب من الفقه القانوني(٢) رأيًا مخالف لهذا الحكم القضائي، حيث ذهبوا إلى أنه لا يمكن القول بقصر صفة العميل على من له حساب لدى البنك، وقد برروا ذلك بأن العمليات المصرفية الالكترونية استحدثت التزاما عامًا يقع على كل من يحصل على أحد الخدمات التي يقدمها البنك بالسرية(٣)، وفي ظل ذلك لا يمكن قصر وصف العميل فقط على من له حساب لدى البنك، وخاصة أن هناك من يتعامل مع البنك دون أن يكون لديه حساب.

ويبدو لنا رجحان رأى الفقه القانوني فيما ذهب إليه من رأى وتبرير، خاصة عند الحديث عن عميل البنك العامل عبر شبكة الإنترنت، وذلك لسببين:

---

(1) **Ross Cranston,** Principles of banking law, second Edition, Oxford university press, 2003, p. 130.

(2) **James E Backhouse**; Op. Cit, p. 30; **Ross Cranston**; Op. Cit, p. 130.

(٣) ويعد إثقال كاهل العميل بهذا الالتزام من مستجدات العمليات المصرفية الإلكترونية؛ حيث اقتضت طبيعة هذه العمليات التعامل عن بعد عبر أجهزة إلكترونية، الأمر الذي فرض على البنك إخبار عميله ببعض البيانات التي تمكنه من الدخول على نظام البنك، والتعامل معه بمقتضى هذه البيانات. ولما كان البنك لا يسمح بالدخول إلى نظامه والتعامل معه إلا من قبل العميل المخول بذلك، فقد فرض على العميل الالتزام بسرية هذه البيانات.

الأول: أن البنك الإلكتروني على شبكة الإنترنت- على خلاف البنك التقليدي- يقدم خدماته عن بعد، الأمر الذي يفرض ضرورة الاستيثاق من شخصية الراغب في التعامل مع البنك، وإلزامه في مواجهة البنك بمجموعة من الالتزامات التي تحكم تعامله مع الموقع الإلكتروني للبنك، والتي من أهمها المحافظة على سرية البيانات الخاصة بالتعامل مع هذا الموقع، وهى التزامات يفرضها البنك على المتعامل معه بوصفه العميل، دون التقيد بوجود حساب له لدى البنك.

الثاني: أن هناك بعض الخدمات المصرفية التي يؤديها البنك لعملائه عبر شبكة الإنترنت، والتي لا تتطلب وجود حساب للعميل لدى البنك، وذلك مثل تحصيل الأوراق التجارية المعالجة إلكترونيا، وأيضا بعض الخدمات الخاصة بالاستشارات المعلوماتية الخاصة بشؤون التجارة والاستثمار(1)، والتي لا يحتاج الأمر بخصوصها إلى وجود حساب خاص بالعميل لدى البنك، خاصة أن دور هذه الخدمات يتعاظم في ظل وجود بنك يعمل ويؤدى خدماته عبر أكبر شبكة معلومات وهى شبكة الإنترنت.

وبناءً عليه يحظى بوصف العميل كطرف مناظر للبنك الإلكتروني في العقد المصرفي أي شخص يطلب أحد الخدمات التي يقدمها البنك عبر شبكة الإنترنت يستوي أن يكون هذا الشخص لديه حساب لدى البنك أم لا.

ويلاحظ أن عميل البنك الإلكتروني يمكن أن يكون بنكًا آخر يطلب من البنك الإلكتروني أحد الخدمات المصرفية التي يقدمها عبر شبكة الإنترنت (خاصة إذا كان هذا البنك لا يقدم خدمات مصرفية إلكترونية)، أو أي شخص سواء كان

(1) **S.K Leong, T. Srikanthan, G. S. Hura**; Op, Cit, p. 3.

تاجرًا أم لا[1].

١٤٢- وبعد التعرف على أشخاص العقود المصرفية على شبكة الإنترنت، نتعرض لتعريف هذه العقود، وذلك من خلال بيان الموقف التشريعي والفقهي، وذلك على النحو التالي:

أولا/ الموقف التشريعي:

١٤٣- لم يظهر لنا تعريف تشريعي خاص بالعقود المصرفية على شبكة الإنترنت. ويمكن أن نرجع هذا الصمت التشريعي لأسباب معينة، أهمها:

أ- حداثة العقود المصرفية على شبكة الإنترنت، بسبب حداثة ممارسة العمليات المصرفية عبر شبكة الإنترنت.

ب- صعوبة حصر العمليات المصرفية على شبكة الإنترنت (باعتبارها محلا لهذه العقود)؛ حيث إنها في حالة زيادة وتطور بشكل مطرد ومستمر، وذلك بفضل ما يتوافر على شبكة الإنترنت من إمكانات سهلت على البنك أن يطور من الخدمات التقليدية، بل ويضيف إليها خدمات ذات طابع معلوماتي وتسوقي لم يكن يعرفها العمل المصرفي من قبل.

وعلى الرغم من أهمية وضع تعريف مناسب للعقود المصرفية على شبكة الإنترنت، إلا أننا نفضل أن تحتفظ التشريعات القانونية بموقفها الصامت تجاه هذا الأمر؛ حيث يصعب حصر العمليات المصرفية وآليات التعاقد عليها في ظل هذا التقدم التقني الهائل في تكنولوجيا الاتصالات والمعلومات، والذي من شأنه أن يفرز لنا أشكالا جديدة من العمليات المصرفية وآليات جديدة لإبرام عقودها

(1)**Ross Cranston**; Op, Cit, p. 129.

وتنفيذها، ومن ثم فأن عدم تدخل المشرع لوضع تعريف هنا من شأنه أن يعطى للبنك الإلكتروني مزيدا من حرية الحركة عند مباشرته لنشاطه، بما يساعده على تطوير خدماته، وإضافة أشكال جديدة لها، بما سينعكس على أدائه. وإن كان هناك منهج وسط يفضل أن تتبناه التشريعات القانونية؛ وهو وضع مجموعة من الشروط تمثل الحد الأدنى لما يجب أن يتوافر في العقود المصرفية، هذه الشروط تعكس وتجسد أهم الخصائص التي يجب أن تتوافر في هذه العقود. وبهذا المنهج يتمكن المشرع من تمييز العقود المصرفية على شبكة الإنترنت عن غيرها من العقود التي تتشابها معها، كما يتمكن أيضا من تفادى ضيق ألفاظ التعريفات ومشاكلها.

ثانيا/ الموقف الفقهى:

١٤٤- وعلى صعيد الفقه القانوني نلاحظ أنه انقسم في تعريف العقود المصرفية على شبكة الإنترنت إلى اتجاهين:

الاتجاه الأول: عدم وضع تعريف للعقود المصرفية على شبكة الإنترنت:

يرى أنصار هذا الاتجاه[١] أن هناك صعوبة في وضع تعريف لهذه العقود، معللين لذلك بسببين:

(أ) اتساع وتعدد الخدمات المصرفية الإلكترونية بصورة مستمرة، الأمر الذي يصعب معه حصرها في تعريف يحكمها.

(ب) تعدد وتنوع الوسائل التكنولوجية التي تستخدم في تقديم مثل هذه الخدمات.

---

(1) **Valters Kaze, Ilona, Erika Sumilo, Roberts Skapars**: Op, Cit. p. 181.

وعلى الرغم من وجاهة هذا الرأي وتبريراته، إلا أنها صعوبة لا يعرفها إلا المشرع، بالنظر إلى ما يرتبه تدخله في مجال التعريفات بصورة عامة، والمصرفية بصورة خاصة من مشاكل تتعلق بضيق وقصر الألفاظ والمصطلحات عن استيعاب المستجدات الخاصة بالنشاط محل التعريف، لكن الأمر على خلاف ذلك بالنسبة لرجال الفقه المجندين دائما لهذه المهمة، خاصة عندما يتعلق الأمر بمسألة جديدة (العقود المصرفية على شبكة الإنترنت) تلح الحاجة في وضع تعريف لها من أجل إيجاد تنظيم قانوني ملائم لها.

الاتجاه الثاني: وضع تعريف للعقود المصرفية على شبكة الإنترنت:

ذهب بعض الفقه إلى ضرورة وضع تعريف للعقود المصرفية على شبكة الإنترنت، حيث ذهب فريق منهم[1] يعرفه بأنه عبارة عن اتصال افتراضي (أي دون حضور مادي) بين العميل والبنك من أجل الحصول على خدمات مصرفية، أو إدارة الأموال المودعة لدى هذا البنك والتحكم فيها.

ذهب فريق آخر[2] إلى تعريفه بأنه عبارة عن عقد يبرم من خلال اتصال العميل بالكمبيوتر المركزي للبنك عبر شبكة الإنترنت، بغرض الحصول على إحدى الخدمات المصرفية، من استلام ودفع الفواتير وغيرها من الخدمات المصرفية.

والملاحظ على هذه التعريفات أنها انشغلت ببيان أسلوب التعاقد، وغفلت عن

---

(1) **Valters Kaze, Ilona, Erika Sumilo, Roberts Skapars,** Op, Cit., p. 181.

(2) **U.S. Consumers and electronic banking, 1995-2003**. available at: www.federalreserve. gov/pubs/bulletin/2004/winter04_ca.pdf.

إبراز الجانب القانوني من تعريف العقود المصرفية على شبكة الإنترنت.

١٤٥- رأينا الخاص:

من جانبنا نؤيد الاتجاه الفقهي الثاني في ضرورة وضع تعريف للعقود المصرفية على شبكة الإنترنت، وذلك للأسباب السابق ذكرها في أهمية هذا الأمر. لكن يبدو لنا ضرورة تأصيل هذا التعريف، بما يتلاءم مع طبيعة الوسيلة المستخدمة لإبرام هذه العقود وتنفيذها (شبكة الإنترنت)، والطبيعة الخاصة للعمليات المصرفية الإلكترونية باعتبارها محلا لهذه العقود.

ومن خلال إمعان النظر في العقود المصرفية على شبكة الإنترنت، نلاحظ أنها لا تعدو أن تكون إحدى صور العقود الإلكترونية التي تتم عبر هذه الشبكة[١]، وذلك بالنظر إلى وسائل إبرامها وطريقة تنفيذها.

ويعرف العقد الإلكتروني على شبكة الإنترنت بأنه اتفاق ما بين شخصين أو

---

(١) فالملاحظ أن هناك خلطًا شائعًا في مفهوم العقود الإلكترونية والعقود الإلكترونية عبر شبكة الانترنت، ويعود ذلك إلى الخلط بين مفهوم كلا من التجارة عبر الانترنت والتجارة الإلكترونية. فمصطلح التجارة الإلكترونية هو ترجمة عبارة E-Commerce، وتستخدم أحيانا كمرادف لعبارة التجارة عبر الانترنت Commerce I- حيث يستخدم كل من المصطلحين كبديل للآخر، في حين أن الثانية من الناحية العملية تعد فرعا ثانويا من الأولى. ويمكن القول بوجه عام أن التجارة الإلكترونية " هى إنجاز الأعمال من خلال صيغة إلكترونية ". في حين أن التجارة عبر الانترنت " هى انجاز الأعمال بصيغة إلكترونية من خلال الانترنت ". ولكن مصطلح التجارة الإلكترونية هو الأكثر شيوعا واستخداما. لذلك يستخدم للدلالة على التجارة عبر الانترنت مجازا. انظر. **بهاء شاهين**، العولمة والتجارة الإلكترونية، الفاروق الحديثة للطباعة والنشر، الطبعة الأولى، ٢٠٠٠، ص٦٢، د. **أسامة أبو الحسن**،مرجع سابق، ص٣٤؛

Julian JB Hickey; Op. Cit, p. 16.

كثر باستخدام شبكة الإنترنت، بغرض إنشاء رابطة قانونية أو تعديلها أو إنهائها(١).

ويلاحظ على تعريف العقد الإلكتروني على شبكة الإنترنت، أنه لا يخرج عن تعريف العقد بصورة عامة إلا من حيث الوسيلة المستخدمة في إبرام العقد وتنفيذه، وهى شبكة الإنترنت.

وبما أن العقود المصرفية على شبكة الإنترنت تنتمي لطائفة العقود الإلكترونية

---

(١) د. **سمير حامد الجمال**،مرجع سابق، ص ٦٤.

- وعلى الرغم من تعرض التوجيه الأوربي الصادر في ٢٠ مايو ١٩٩٧ لتعريف التعاقد عن بعد Remote Contract، إلا أن التوجيه الأوربي الخاص بالتجارة الإلكترونية بتاريخ ٨ يونيه لسنة ٢٠٠٠ والذي يعد مكملاً للتوجيه الصادر في ٢٠ مايو ١٩٩٧ جاء خلوًا من بيان محدد لمفهوم وطبيعة العقد الإلكتروني. انظر مزيدا من التفصيل في تعريف التعاقد عن بعد. د. **محمد حسن قاسم**، التعاقد عن بعد، دار الجامعة الجديدة للنشر، ٢٠٠٥، ص ١٧ وما بعدها؛ انظر أيضا

- هذا وقد تعددت الاتجاهات التي تناولت هذا العقد بالتعريف، حيث عرفه البعض بأنه عبارة عن "اتفاق يتلاقى فيه الإيجاب بالقبول على شبكة دولية مفتوحة للاتصال عن بعد وذلك بوسيلة مسموعة ومرئية، بفضل التفاعل بين الموجب والقابل" **د.أسامة أبو الحسن مجاهد**، مرجع سابق، ص٣٩ وفى نفس المعنى **د. محمد حسين منصور**، مرجع سابق، ص ١٨، وفى نفس المعنى **د. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، مرجع سابق**، ص ٥٢

- وعرفه جانب آخر بأنه "عبارة عن تقابل لعرض مبيعات أو خدمات يعبر من خلال شبكة دولية للاتصالات عن بعد، مع قبول يظهر باستعمال النشاط الحواري بين الإنسان والمعلومة التي تقدمها الآلة". **د.إيمان مأمون، مرجع سابق**، ص ٥٠.

- كما عرف بأنه "ذلك العقد الذي يعقد من خلال الدخول على شبكة الانترنت والذي يتم إثباته بالوسائل الإلكترونية (التي يتم الحصول عليها من ذاكرة الكمبيوتر) بدلاً من الشكل المطبوع"

Roger Gerleroy Miler – Gaylord A. Jentz; Op. Cit, p.146

والملاحظ على هذه التعريفات أنها انشغلت ببيان الوسيلة التي يبرم بها العقد الإلكتروني عبر شبكة الانترنت، وغفلت عن الأثر القانوني المستهدف من تلاقي الإيجاب بالقبول.

على شبكة الإنترنت، فلن تخرج عن إطار هذه العقود إلا فيما يتعلق بخصوصيات التعامل المصرفي. لذلك نرى أن تعرف العقود المصرفية على شبكة الإنترنت بأنها عبارة عن تلاقي الإيجاب والقبول لكل من البنك الإلكتروني والعميل عبر شبكة الإنترنت بهدف إنشاء رابطة عقدية أو تعديلها أو إلغائها فيما يتعلق بإجراء إحدى العمليات المصرفية الإلكترونية؛ مثل عمليات الإيداع والسحب وعمليات الائتمان وإصدار النقود الإلكترونية، والتحويل المصرفي الإلكتروني وغيرها من العمليات المصرفية الإلكترونية.

المطلب الثاني

خصائص العقود المصرفية على الإنترنت

١٤٧- كما سبق أن ذكرنا، يمثل تحديد خصائص العقود المصرفية على الإنترنت أهمية خاصة، بإعتبارها الحد الأدنى من المواصفات التي يجب أن تتوافر في هذه العقود، والذي يجب أن يعالجه المشرع بنصوص خاصة، وذلك تفاديا لاختلاطها بغيرها من عقود الخدمات المالية التي تقدم على شبكة الإنترنت. يضاف إلى ذلك أنه هذه الخصائص يرتبط بها مجموعة من الآثار القانونية التي يجب أن تؤخذ في الاعتبار.

وتجدر الإشارة إلى عدم تنظيم المشرع المصري لخصائص العقود المصرفية على الإنترنت، الأمر الذي يشكل فراغا تشريعيا في واحدة من أهم المجالات التي تحتاج إلى معالجة قانونية.

ويمكن القول، بأنه على الرغم من تعدد وتنوع العقود المصرفية على شبكة الإنترنت ــ بتنوع الخدمات المصرفية الالكترونية ــ إلا أنها تتميز بمجموعة من الخصائص التي تعد بمثابة قاسم مشترك فيما بينها، والتي لا يمكن وضع نظام قانوني يحكم وينظم هذه العقود دون أخذ هذه الخصائص في الاعتبار. ومن أهم هذه الخصائص:

(١) وجود الوسيط الإلكتروني للاتصال عن بعد:

١٤٨- تتميز العقود المصرفية على شبكة الإنترنت بهيمنة الوسيط الإلكتروني على مجريات إنشاء العقد وتنفيذه[1]، والمقصود بالوسيط الإلكتروني في هذا الخصوص شبكة الإنترنت بكل ما تشتمل عليه من أجهزة وأدوات إلكترونية، حيث يعتمد البنك على هذه الشبكة في الإعلان عن الخدمات المصرفية، وفي التعاقد من خلالها مع عملائه، وحتى تمام تنفيذ الخدمة المطلوبة[2].

ويترتب على ذلك أنه لا مجال لوجود أي وثائق ورقية متبادلة في إجراء وتنفيذ العقود المصرفية على شبكة الإنترنت، حيث إن كافة مراحل التعاقد على الخدمة المصرفية تتم إلكترونيا[3].

ومع ذلك، لا يخل من هيمنة الوسيط الإلكتروني على مجريات التعامل بين البنك وعميله، تلقى الأخير بعض الأدوات التي تمكنه من الحصول على الخدمة بصورة مادية؛ فاستلام العميل كرت الدفع الإلكتروني بصورة مادية لاستخدامه

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 10; **Is auditing guideline internet banking**; Op. Cit, p. 2.

(٢) **د. على أحمد مرسى عثمان**، مرجع سابق، ص٤٣.

(٣) **رأفت رضوان**، مرجع سابق، ص ١٧.

في عملية الدفع، لا ينتقص من الوصف الإلكتروني للمعاملة، حيث إن التعاقد بخصوص هذه الخدمة، وتنفيذها (من خلال تمكين البنك لعميله استخدامها في عمليات الدفع الإلكتروني) يتم بصورة إلكترونية، ولا يعد هذا الاستلام سوى أثر تابع لتنفيذ الخدمة.

وتتميز العقود المصرفية على شبكة الإنترنت بالإضافة لكونها عقود إلكترونية، أنها تتم عبر وسيلة للاتصال عن بعد(١).

وقد تضمن التوجيه الأوربي الصادر في ٢٠ مايو ١٩٩٧ تعريفا للعقد عن بعد "Remote Contract" بأنه أي عقد متعلق بسلع أو خدمات يتم بين المورد والعميل من خلال الإطار التنظيمي الخاص بالبيع عن بعد أو تقديم الخدمات التي ينظمها المورد، والذي يتم باستخدام واحدة أو أكثر من وسائل الاتصال الإلكترونية (Remote Communication)، حتى إتمام التعاقد"(٢).

---

(١) واصطلاح **الاتصال عن بعد** يعنى فنيا بالمعنى الواسع، كل نوع أو نموذج لشبكة معنية بالاتصالات السلكية أو اللاسلكية، أو الاتصالات الترددية، أو الاتصال بالأقمار الصناعية، مثل شبكة الانترنت، فهي شبكة مفتوحة للجمهور، ويتم إبرام العقد الإلكتروني عبرها بين أشخاص غير حاضرين، وهذا ما يميز عقد التجارة الإلكترونية عن عقد التجارة العادية. انظر د. **فريد عبد المعز فرج**، التعاقد بالانترنت، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون- فرع دمنهور، العدد الثامن عشر، الجزء الأول ١٤٢٤هـ - ٢٠٠٣ م ص٤٨٨

- كما عرف **الاتصال عن بعد** في المادة الثانية من القانون الفرنسي رقم ٨٦ -١٠٦٧ الخاص بحرية الاتصال بأنه عبارة عن " كل انتقال أو إرسال أو استقبال لرموز أو إشارات أو كتابة أو أصوات أو معلومات أيا كانت طبيعتها، بواسطة ألياف بصرية أو طاقة لا سلكية أو أية أنظمة إلكترومغناطيسية أخرى. د. **سمير حامد الجمال**، ص١٤٥؛ د. **محمد حسن قاسم**، مرجع سابق، ص١٧

(2) **Directive 97/7/EC,** Official Journal of the European Communities, 20 May 1997 (on the protection of consumers in respect of distance contracts), Article 2. available at: www.spamlaws.com/docs/97-7-

كما تضمنت الفقرة الثانية من ذات التوجيه تحديدا لوسائل الاتصال عن بعد، بأنها " كل وسيلة تستخدم للاتصال عن بعد بدون حضور مادي متزامن لمقدم الخدمة والعميل، وتؤدى إلى إبرام العقد".

ويتضح من هذه النصوص أن هناك شرطين للقول بأن التعاقد عن بعد، وهما:

أ) عدم الحضور المادي لأطراف العقد أثناء التعاقد.

ب) أن يتم إبرام العقد بوسيلة من وسائل الاتصال الإلكتروني.

وتتحقق هذه الشروط في العقود المصرفية على شبكة الإنترنت؛ حيث يتعامل البنك مع عميله بدون التقاء مادي فيما بينهما سواء في وقت إبرام العقد أم وقت تنفيذه، كما أن شبكة الإنترنت تأتى على رأس وسائل الاتصال الإلكتروني. وبناء عليه تعد العقود المصرفية على شبكة الإنترنت عقودًا عن بعد.

هذا وقد كان لشبكة الإنترنت كوسيلة إلكترونية للتعاقد المصرفي عن بعد بالمعنى السابق العديد من الفوائد التي عادت على كل من البنك وعملائه، أهمها[1]:

أ- **سهولة إبرام وتنفيذ العقود المصرفية**، فلم يعد مطلوبا من العميل التواجد في مبنى البنك والقيام بكتابة البيانات الخاصة بالعقد المصرفي، حيث يكفي في ظل التعامل عبر شبكة الإنترنت أن يقوم العميل بالضغط على بعض المفاتيح أو

---

ec.pdf

(1) **Valters Kaze, Ilona, Erika Sumilo, Roberts Skapars**: Op, Cit, p. 178; **Zakaria I.Saleh;** Op, Cit, p. 14;**G C Chalikias;** Op, Cit. p. 2

الأيقونات لإبرام العقد، بدون أن يبرح مكانه [1].

ب- **الاقتصاد في النفقات**، حيث يستطيع البنك التواصل مع عملائه عن طريق موقعه الإلكتروني على شبكة الإنترنت، والذي يعد بمثابة نافذة يطل البنك من خلالها على العالم بأسره لتقديم خدماته المصرفية. فلم يعد البنك بحاجة إلى مباني وأجهزة، ومعدات وموظفين كأدوات للتعاقد مع العملاء، الأمر الذي يوفر على البنك كل هذه النفقات للتعاقد مع العملاء بما يزيد من ربحيته[2]. أيضا يستطيع العميل أن يوفر نفقات الانتقال إلى مقر البنك، والانتظار في صفوف مكتظة بالعملاء، ليحصل على الخدمة المطلوبة[3].

ج- **تعدد وتنوع العقود المصرفية الإلكترونية**، بسبب تنوع وتعدد العمليات المصرفية محل هذه العقود. فشبكة الإنترنت مكنت البنك ليس فقط من تنويع أساليب تقديم الخدمة المصرفية، ولكن أيضا إضافة أشكال جديدة من الخدمات لم

---

(1) **Jeanette Taft**; Op, Cit, p. 2.

(2) **Gautam Ivatury, Mark Pickens**;Op, Cit, p. 233; **Jeanette Taft**; Op, Cit, p. 3; **Olga Lustsik**; Op, Cit, p. 18; **Valters Kaze, Ilona, Erika Sumilo, Roberts Skapars**; Op, Cit, p. 177.

(٣) وقد أجريت دراسة في الولايات المتحدة الأمريكية عن مسألة توفير نفقات العميل في حالة قيامه بالتعامل مع البنوك الإلكترونية، حيث ثبت خلالها أن أحد الخدمات المصرفية التي يحصل عليها العميل في حالة تعامله مع البنوك التقليدية تقدر ١,٠٧ دولار، في حين أن تكلفة الحصول على ذات الخدمة من قبل بنك إلكتروني تقدر ٠,٥٤ دولار؛

Valters Kaze, Ilona, Erika Sumilo, Roberts Skapars; Op, Cit, p181; **Kari Liuhto-Olga Lustsik- Mart Sorg- Janek Uiboupin**, Organizational and sectoral changes in transition banking: Estonian experience, Journal of the humanities & Social sciences, 2007, p. 167; **Garcia, Erica**, What's left of the online banks, Academic search premier, Oct 2001, Vol. 30, Issue 10, p.1.

تكن موجودة من قبل (كإصدار النقود الإلكترونية عبر شبكة الإنترنت، وخدمات الاستثمار، والتسوق الإلكتروني)(١)، أيضا كان لشبكة الإنترنت الدور الأكبر في تمكين البنك الإلكتروني من تنويع وسائل التعاقد الخاصة بهذه الخدمات مثل العقود النموذجية والبريد، الإلكتروني(٢).

١٤٩- ويترتب على وصف العقود المصرفية على شبكة الإنترنت بأنها عقود إلكترونية عن بعد مجموعة من الآثار القانونية، أهمها:

(أ) يجب على البنك أن يحدد الطبيعة القانونية لما يصدر عنه من إعلانات خاصة بالخدمات المصرفية التي يقدمها، أو ما يقوم بعرضه من نماذج للعقود الخاصة بخدماته المصرفية، وذلك بأن يؤكد على أن ذلك مجرد دعوة للتعاقد لا يكفى قبولها من قبل العميل لانعقاد العقد، بل يجب إذا ما وافق الأخير على ما ورد في العقد من شروط أن يوجه ابتداء إيجابا للبنك، على أن يقبل أو يرفض البنك. أيضا يجب أن يوضح البنك أن ما يصدر عن العميل من تصرفات يريد من ورائها التعبير عن إرادته (كالنقر على الأيقونة المخصصة لذلك في نموذج العقد، أو إرسال بريد إلكتروني) قبولا في خصوص هذه العقود من عدمه(٣). ويبرر ذلك بطبيعة التعاقد، وكونه يتم عن بعد عبر شبكة الإنترنت، التي يغيب معها الحضور المادي للمتعاقدين، في وقت تعظم فيه العقود المصرفية من أهمية الاعتبار الشخصي للعميل، وضرورة التأكد من ضماناته المالية التي تؤهله للحصول على إحدى

---

(1) **Haibo Huang**, Op. Cit, p. vii; **Olga Lustsik**; Op, Cit, p. 5.

(2) **N. stephan Kinsella, Andrew F. Simpson**, Online contract formation, Oceana Publications, first edition, 2004, p. 13.

(٣) **د. سمير حامد عبد العزيز الجمال**، مرجع سابق، ص ١٠٥

خدمات البنك.

(ب) الاعتماد على الوسائل الإلكترونية(شبكة الإنترنت) في إنشاء العقد المصرفي وتنفيذه ينعكس على إثبات هذا العقد، وذلك على النحو الذي يمكن معه القول بأن الإثبات يكون من جنس العمل. ولما كان هذا الأخير إلكترونيا فإن إثبات كل ما يتعلق بهذا العقد يكون بمقتضى المخرجات الإلكترونية[١].

(ج) يجب على البنك اتخاذ كافة الإجراءات اللازمة لتأمين تعاقداته المصرفية على شبكة الإنترنت، كالتزود بالأدوات التي تمكنه من التعرف على شخصية المتعاقد معه، والتأكد من أهليته القانونية للتعاقد، فالتعاقد يتم بدون حضور مادي لأطرافه، الأمر الذي يحتم ضرورة استعانة البنك بالوسائل التي تمكنه من التعرف على هوية هذا المتعاقد. ومن أهم الوسائل التي يمكن للبنك أن يعتمد عليها في ذلك، ما هو مرتبط بشخص المتعاقد؛ كالخواص البيومترية (كاتساع حدقة العين والطول الموجي للصوت)، ومنها ما يعتمد على بيانات خاصة بالمتعاقد (مثل كلمة المرور)، وحديثا يتم اللجوء لبعض الوسائل التي تعتمد على ما يحوزه المتعاقد؛ مثل الكروت الذكية التي يستخدمها في عمليات الدفع[٢]. يضاف إلى ذلك ضرورة تأمين موقع البنك،

---

(١) **د. بلال عبد المطلب بدوى**، البنوك الإلكترونية، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص١٩٥٢.

(2) **Gabriele Lenzini, Mortaza S. Bargh and Bob Hulsebosch**, Trust- enhanced security in location-based adaptive authentication, Electronic notes in theoretical computer Science 197), 2008, p. 106; **Apostolos Ath. Gkoutzinis**; Op. Cit, p.187; **Roger Dean**, Identity management back to the user, Network Security puplish-ment, December 2006, p. 4.

ومعاملاته المصرفية ضد كل محاولات الاطلاع غير المشروع، أو التلاعب في الملفات الموجودة على قاعدة البيانات الخاصة بالبنك، الأمر الذي يعظم من ضرورة الاستعانة بوسائل تأمين خاصة تتناسب مع طبيعة البيئة الإلكترونية، وطبيعة العقود المصرفية، مثل التشفير والتوثيق الإلكتروني[١].

ونظرا للأهمية القصوى لتنظيم استعانة البنك بوسائل التأمين المناسبة، فسوف نعرض لهذا الأمر تفصيليا في الباب الثالث من هذه الدراسة، بإذن الله[٢].

(٢) العقود المصرفية على الإنترنت ذات طابع دولى:

١٥٠- تعد هذه الخاصية من مستحدثات العمل المصرفي على شبكة الإنترنت، حيث لم تكن تعرفها العقود المصرفية التقليدية(إلا في حالات بسيطة). فقد مكنت شبكة الإنترنت البنك بفضل اتساع نطاقها وربطها لأطراف العالم المترامية من مخاطبة كل دول العالم بخدماته[٣]، الأمر الذي أسبغ الصفة الدولية على عقوده[٤].

---

(١) **د. إسماعيل شاهين**، أمن المعلومات في الانترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون- جامعة الإمارات العربية المتحدة، من ١- ٣ مايو ٢٠٠٠، ص ٧؛ **د. على أحمد مرسى عثمان**، مرجع سابق، ص ٤٤.

Simon Newman and Gavin Sutter, electronic payments- the smart card, law - part I Computer Law & Security Report, Vol. 18 no. 4, 2002, p 237; **Graham Smith**; Op. Cit, p. 278; **Thomas C. Glaessner, Tom Kellermann, Valerie Mc Nevin**; Op. Cit, p. 71; **Electronic money**; Op. Cit, p. 12

(٢) انظر لاحقا، ص ٤١٦.

(3) **Jeanette Taft**;Op, Cit, p. 3.

(4) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 10.

ويجب ملاحظة أن الصفة الدولية ملازمة للعقود المصرفية علـــى الإنترنـــت، سواء كانت إقامة العميل ومركز أعماله في ذات إقليم البنك، أم في إقليم آخـــر. ويعود ذلك إلى غياب مفهوم الحدود الجغرافية بمعناها التقليدي في التعامل عبر هذه الشبكة، فالأخيرة كما ينظر إليها بعض الفقهاء(١) ـــ وبحق ـــ نظام دولي لا يمكن رده إلى دولة بعينها. فلو أن البنك يحمل الجنسية المصرية، وكان العميـــل متواجدا في مصر أثناء التعاقد، لا يمكن في ظل ذلك القول بأن مصر هي مكان إبرام العقد، بل مكان إبرامها شبكة الإنترنت ذات الطبيعة الدولية.

ولا شك في أن دولية العقود المصرفية الإلكترونية، بهذا المعنى من شأنها أن

- لذلك يذهب البعض وبحق إلى أن شبكة المعلومات الدولية (Internet) هي التي أنتجت عولمة الاقتصاد والمجتمعات ومن ثم المعاملات التي تجرى في إطارها، وذلك بسبب ما أتاحته من إنشاء سوق إلكترونية كبيرة تضم دول العالم بأسره، وذلك بعيدا عن كافة القيود والعوائق الحكومية التي تفرضها الدول على إجراء المعاملات الدولية. انظـــر د.**عـــزت محمد على البحيرى**، القانون الواجب التطبيق علـــى المعـــاملات الإلكترونيـــة، مـــؤتمر الأعمال المصرفية الإلكترونية بين الـــشريعة والقـــانون، ٩-١١ ربيـــع الأول ١٤٢٤هـ الموافق ١٠- ١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص ١٦٦٨؛ انظر أيضا د. **أحمد الهوارى**، عقود التجارة الإلكترونية في القانون الدولي الخاص، مـــؤتمر الأعمـــال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ هـــ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص١٦٤٥.

Is auditing guideline internet banking; Op. Cit, p. 2

Kit Burden; Op. Cit, p. 251

(١) ويرى البعض في سبيل تأصيل هذه الفكرة إلى القول، بأن الأسس التي يقـــوم عليهـــا منهج تنازع القوانين، والذي يعتمد على أماكن تواجد الأشخاص والمنشآت الوطنية في الإقليم الوطني، أصبحت لا تتناسب مع طبيعة شبكة الانترنت، التي لا تقـــدر طبيعـــة الروابط الطبيعية بين الأشخاص القانونيين وأماكن تواجدهم. د. **عادل أبـــو هـــشيمة محمود حوته**، عقود خدمات المعلومات الإلكترونية في القانون الدولي الخـــاص، دار النهضة العربية، ٢٠٠٤، ص ٥٨؛ د.**عزت محمد على البحيرى**، مرجع ســـابق، ص ١٦٦٩.

تعظم من الفوائد التي يمكن أن يجنيها البنك؛ حيث تتسع قاعدة عملائه، بالنظر إلى قدرته من تقديم خدماته لأي شخص في أي دولة من دول العالم(١).

١٥١- وعلى الرغم من هذه الفوائد، إلا أن دولية العقود المصرفية على الإنترنت، تتسبب في العديد من المشاكل القانونية، التي يجب على البنك أن يواجهها، وهو بصدد تنظيم شروط وبنود هذه العقود. ومن أهم هذه المشاكل:

أ) دولية العقد المصرفي من شأنها أن تتعارض مع مبالغة البنك الإلكتروني في مراعاة الاعتبار الشخصي للعميل، حيث يجد البنك صعوبة- خاصة إذا كان العميل ينتمي لدولة أجنبية(٢)- في التحقق من مفردات هذا الاعتبار؛ كالتأكد من المركز المالي للعميل، ومشروعية أمواله (ليست متحصلة من غسيل أموال(٣)). أيضا دولية هذا العقد تؤدى إلى إثارة مشكلة القانون الواجب التطبيق، والمحكمة المختصة بنظر النزاع، نظرا لوجود العنصر الأجنبي في العلاقة(٤).

ويمكن للبنك أن يتفادى مثل هذه المشاكل عند صياغته للعقود المصرفية التي تنظم تقديم خدماته، بأن يستعين بجهات التوثيق الإلكتروني للتعرف على

---

(1) **Jeanette Taft**;Op, Cit, p. 3.

(2) **Zakaria I. Saleh** ; Op, Cit, p. 14.

(٣) **د. محمد عبد السلام محمد**، جرائم غسيل الأموال إلكترونيا في ظل النظام العالمي الجديد للتجارة الحرة (العولمة)، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص ١٥٠٩؛ **د. صفوت عبد السلام عوض الله**، الآثار الاقتصادية لعمليات غسيل الأموال ودور البنوك في مكافحة هذه العمليات، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص ١٥٤٤.

(٤) **د. أحمد الهوارى**، مرجع سابق، ص ١٦٤٧.

شخصية العميل الذي يريد التعامل مع البنك، والتأكد من ملاءته المالية التي تؤهله لذلك(١). أيضا يراعى عند صياغة العقود المصرفية أن يحدد القانون الواجب التطبيق على هذا العقد، والمحكمة المختصة بنظر ما قد ينشأ من منازعات(٢).

هذا وقد سعى الاتحاد الأوربي إلى تجنب المشاكل المتعلقة بتنازع القوانين، وتحديد المحكمة المختصة بنظر النزاع، من خلال إيجاد نوع من التوحيد بين التشريعات الوطنية للدول. وقد كان سبيله إلى ذلك وضع توجيهات عامة تحكم إبرام العقود المصرفية على شبكة الإنترنت، وتحمي المستهلك الإلكتروني في هذه العقود من الشروط المجحفة Unfair Terms(٣).

ب) أن دولية العقد المصرفي قد تصطدم ببعض العقبات في النظم القانونية الداخلية. فبعض الدول تشترط- لاعتبارات قانونية وثقافية- التعبير عن

(1) **CMS Information Systems Threat Identification Resource,** Center for medicare& medicaid services, version 1.0, May 7, 2002, p 7, available at: http://csrc.nist.gov/fasp/ FASPDocs/risk-mgmt/Threat_ID_resource.pdf

(2) **Michael Chissick, Alistair Kelman**; Op. Cit, P. 115.

(3) **Directive 93/13/EEC,** (unfair terms in consumer contracts), Official Journal of the European Communities, 5 April 1993, , available at: ec.eurOpa.eu/consumers/policy/ develOp-ments/unfa_cont_term/uct01_en.pdf

- هذا وقد وجدت الدول الأعضاء في الاتحاد الأوربي أن اختلاف التشريعات الوطنية المنظمة للعلاقات التعاقدية الخاصة بالتعاملات المالية من شأنه أن يزيد من تكلفة الصفقات العابرة للحدود، بما ينعكس على تكاليف تشغيل المؤسسات المالية المقدمة للأنشطة المالية، وقد كان سبيله إلى ذلك استبدال القانون المدني الأوربي الموحد بالقوانين المدنية الأوربية، والقانون الأنجلوسكسوني العام.

Apostolos Ath. Gkoutzinis; Op, Cit, p. 184.

الإيجاب بلغتها الوطنية في العقود التي تبرم مع أحد مواطنيها، وذلك أيا كان الأسلوب المتبع للتعبير عن هذا الإيجاب (وسائل تقليدية أم إلكترونية)[1]. ومن هذه الدول فرنسا، حيث أوجب قانون **Toubon** (الصادر في ١٩٩٤/٨/٤) استعمال اللغة الفرنسية للتعبير عن الإيجاب في كل أنواع المعاملات (ومنها معاملات التجارة الإلكترونية) خاصة عند وصف الخدمة أو السلعة، والإيجاب الخاص بها، وتعيين نطاقه وماله من ضمان وكذلك في طريقة التشغيل أو الاستعمال للوسائل الإلكترونية[2].

وقد سعى المشرع الفرنسي من وراء إصدار مثل هذا القانون إلى حماية المستهلك الفرنسي وذلك من خلال مساعدته على فهم كل مواصفات السلعة وشروط التعاقد الخاصة بها بسهولة ويسر[3].

وتظهر مشكلة نص كهذا في خصوص العقود المصرفية على شبكة الإنترنت، في تمكين العميل الفرنسي من التمسك في مواجهة البنك الإلكتروني ببطلان العقد المصرفي بموجب قانون Toubon لكونه استعمل لغة غير الفرنسية في تقديم خدماته. على الرغم من أن هذا يتنافى مع الطبيعة الدولية لهذه العقود، ومن شأنه أن يحرم البنك الإلكتروني من الاستفادة من مميزات التعامل عبر شبكة دولية كشبكة الإنترنت. كما أنه يتنافى مع الأصول القانونية التي تواترت على عدم اشتراط التعاقد بلغة معينة.

---

(١) **توفيق شمبور**، مسائل قانونية خاصة بالتجارة الإلكترونية، مجموعة بحوث التجارة الإلكترونية والخدمات المصرفية والمالية عبر الانترنت، اتحاد المصارف العربية، ٢٠٠٠، ص ٨.

(2) **Nicole Atwill** ; Op, Cit, p. 7.

(٣) **إيمان مأمون سليمان**، مرجع سابق، ص ١٣٢

هذا وقد تداركت الحكومة الفرنسية هذا الأمر سريعا، بمنشور صدر عنها في ١٩ مايو ١٩٩٦[١]. يخفف من غلواء قانون Toubon، حيث ذهبت الحكومة إلى وجوب استخدام اللغة الفرنسية في كتابة البيانات على الشاشات الإلكترونية مع جواز اقترانها بترجمة إنجليزية أو أي لغة أجنبية أخرى.

وقد ذهب جانب من الفقه[٢]. في سبيل وضع علاج لمواجهة مثل هذه المشكلة في حالة وجودها، إلى أنه يجب أن يكون هناك اتفاق دولي على أن يكون الإيجاب في التعاقد عبر شبكة الإنترنت بإحدى اللغات العالمية الرئيسة التي يستعملها معظم سكان الكرة الأرضية، والجائزة كلغة عالمية أولى من قبل منظمة الأمم المتحدة (كالإنجليزية)، مع إمكان أن يصاحب هذه اللغة ترجمة باللغة الثانية عالميا (وهى الفرنسية) فبذلك تتوحد لغة التخاطب على شبكة الإنترنت.

ونرى من جانبنا أن هذا الوضع وإن كان من الممكن قبوله في التجارة التقليدية، فإنه من الصعب التسليم به في التجارة الإلكترونية خاصة لو تمت عبر شبكة الإنترنت، تلك الشبكة التي يغيب عنها مركزية السلطة، ومن ثم عدم مركزية القوانين الحاكمة للتصرفات.

كما أن ما يصدر عن الهيئات الدولية والإقليمية (منظمة الأمم المتحدة، البرلمان الأوربي) في هذا الخصوص ما هو إلا قوانين نموذجية لا تحمل طابعًا ملزمًا للدول الأعضاء. إلا أننا نرى حلاً لهذه المشكلة يتمثل في قيام البنك الإلكتروني بوضع شروط في عقوده المصرفية التي يجريها على شبكة الإنترنت

(١) د.**أسامة أبو الحسن**، مرجع سابق، ص٧٤.
(٢) د.**فريد عبد المعز فرج**، مرجع سابق، ص٥٣٢.

ينص من خلالها على أن يكون التعاقد وكل ما يتعلق بــه مــن مراســلات أو مخاطبات بلغة معينة، بحيث يكون هذا الشرط جزء لا يتجزأ من هذا العقد، على نحو يمكن معه للعميل أن يكون على دراية بهذه اللغة قبل التعاقد، بحيث إنه إذا قبل التعاقد على هذا النحو فلا يمكن له بعد ذلك أن يتمسك بنص في قانون دولته يوجب التعاقد بلغة معينة، حيث لا يعمل بحكم هذا النص (والذى غالبا ما يكــون من النصوص التكميلية التي يمكن الاتفاق على مخالفتها) متى وجد اتفاق بغيــر ذلك بين المتعاقدين.

ويضيف البعض إلى ذلك أن وضع شرط كهذا من قبل البنك الإلكتروني من شأنه أن يساعده على الحد من دولية شبكة الإنترنت، وذلك بقصره التعاقد علــى طوائف معينة تجيد هذه اللغة[1].

(٣) العقود المصرفية على الإنترنت عقود نموذجية:

١٥٢- يعرف العقد النموذجي (أو النمطي) بأنه العقد الذي يعد في صورة نموذج ينفرد أحد أطرافه بإعداد بنوده، ولا يقبل فيه تفاوضا من قبل الطــرف الآخــر، الذي ليس له إلا أن يقبل العقد كما هو أو يرفضه.

هذا وقد درج عمل البنوك عامة على الاعتماد على العقــود النموذجيــة فــي معاملاتها المصرفية، لاعتبارات تتعلق بالسرعة والسهولة التــي تقــوم عليهــا

(١) د. أسامة أبو الحسن، مرجع سابق، ص ٧٠ وما بعــدها، د. علــى أحمــد مرســى عثمان، مرجع سابق، ص ٤٢، د. سمير حامد عبد العزيز الجمال، مرجع ســابق، ص ١١؛

Michael Chissick, Alistair Kelman; Op. Cit, p. 82; Julian JB Hickey; Op. Cit, p. 213.

المعاملات التجارية بصورة عامة والمصرفية بصورة خاصة(١).

ويكتسب التعاقد النموذجى أهمية خاصة في العقود المصرفية على الإنترنت(٢). ويعود ذلك لسببين:

الأول: هو طبيعة الوسيلة المستخدمة في التعاقد، وهي شبكة الإنترنت وكونها وسيلة إلكترونية للاتصال عن بعد، يغيب في ظلها الالتقاء المادي للبنك بعميله، ومن ثم يصعب فيها التفاوض، الأمر الذي يجعل التعاقد النموذجى هو ضالة البنك الإلكتروني المنشودة، كوسيلة ملاءمة لطبيعة البيئة التي يحيا فيه البنك ويقدم خدماته(٣).

الثاني: زيادة اعتبارات السرعة والسهولة في تقديم الخدمة المصرفية. فالفلسفة التي تقف وراء تبنى التعاقد المصرفي على الإنترنت تتجاوز حدود الترف الاقتصادي، إلى وجود رغبة قوية في التخلص من الروتين القائم في البنوك التقليدية، والتناغم مع الإيقاع السريع للتجارة على الإنترنت، الأمر الذي يعظم من أهمية اعتماد البنك على العقود النموذجية في التعامل مع عملائه.

١٥٣- ويجرى العمل بهذه العقود من خلال قيام البنك بصياغة العقود المصرفية الخاصة بكل خدمة مصرفية، والذي يتضمن جميع شروط العقد والتزامات الطرفين، ويجعله متاحًا على موقعه على شبكة الإنترنت، وعلى العميل إذا ما أراد الحصول على هذه الخدمة المصرفية أن يقوم بالاطلاع على هذه الشروط والتي أعدها البنك سلفا فإذا وافق على الحصول على هذه الخدمة بهذه الشروط

---

(١) د. **عبد الرحمن قرمان**، مرجع سابق، ص ١٠٢.

(2) Apostolos Ath. Gkoutzinis ;Op, Cit, p. 191.

(٣) **د.** على **أحمد مرسى عثمان**، مرجع سابق، ص ٤٢

قام بالضغط على الأيقونة التي تفيد موافقته على العقد، أو لا يوافق على شروط العقد فيرفضه ومن ثم لا يتم إبرام العقد.

وعلى الرغم من فوائد التعاقد النموذجي بالنسبة للبنك على شبكة الإنترنت، إلا أن اتباع البنك لهذا الأسلوب في التعاقد يلقى على عاتقه بمسؤولية كبيرة تتمثل في أن البنك عند صياغته لشروط العقد يجب ألا يكتفي بمجرد سرد شروط العقد وبنوده وفقط (كما هو الحال في العقود المصرفية التقليدية)، بل يجب عليه أن يلحق بكل بند شرحا وتوضيحا وافيا، على النحو الذي يجعل العميل على بينة ودراية بكل تفصيلات العقد. بل يجب أن يمنح البنك للعميل الفرصة الكافية للاطلاع على هذه البيانات، وبطريقة سهلة تمكنه من ذلك[١]. ويبرر ذلك التعاقد عن بعد، بما يستتبعه من غياب الفرصة أمام العميل للتساؤل والاستيضاح، الأمر الذي يجب أن يراعيه البنك، وذلك في إطار التزامه بإعلام العميل[٢].

وقد أكد قانون البنوك الإنجليزي هذا الأمر، بل إنه زاد من هذا التأكيد في حالة إذا ما تضمن العقد شروطا شاقة (Onerous conditions) على العميل، كتلك التي تحرمه من أحد حقوقه القانونية (Deprive the customer of legal right)[٣]، كحقه في الانسحاب من العقد المصرفي بعد إبرامه خلال مدة معينة (Right of withdrawal)[٤]، وحقه في معرفة أسباب فسخ التعاقد بصورة مبتسرة البنك التعامل معه، حيث أعطى له الحق في المطالبة بإبطال العقد.

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 193.
(2) **S.K Leong, T.Srikanthan, G.S.Hura**; Op, Cit p. 3.
(3) **Michael Chissick, Alistair Kelman**; Op. Cit, p. 100.
(4) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 19٠.

ويمكن للبنك الإلكتروني أن يستعين بوصلات إلكترونية Hyperlink[1] لبعض الشروط أو البنود التي تحتاج منه إلى استفاضة في الشرح والتوضيح، حيث تعمل هذه الوصلات على ربط هذا الشرط بصفحة معينة تحتوى على معلومات مفصلة عنه. أيضا يجب على البنك الإلكتروني أن يصمم الصفحات الخاصة بهذه العقود على نحو يسهل معه على المتعاقد قراءة هذه الشروط واستعراضها، وذلك من خلال تزويد هذه الصفحات بأيقونة (Scrolling) خاصة تسمح بتحريك الصفحة بسهولة[2].

وقد اعتمد الإتحاد الفيدرالي للبنوك في ألمانيا بعض نماذج للعقود التي تنظم علاقة البنك الإلكتروني بعملائها[3]. ويجرى العمل أيضا في المملكة المتحدة وفرنسا بأسلوب التعاقد النموذجي[4].

وقد تم تنظيم هذه العقود في صورة شروط عامة وشروط خاصة، حيث تنظم الشروط العامة الإطار العام الذي يحكم علاقة البنك بالعميل، والتي تكاد لا

---

(١) وهى عبارة عن مؤشرات توجد داخل صفحة الويب، وتعمل على ربط هذا المؤشر بصفحات ويب أخرى أو بمواضع أخرى داخل ذات الصفحة بمجرد الضغط على هذا المؤشر. انظر د. **طارق عبد العال، التجارة الإلكترونية**، مرجع سابق، ص٧٨٩.

(2) **Michael Chissick, Alistair Kelman**, Op, Cit, p. 101.

(٣) راجع نماذج لهذه العقود على المواقع الإلكترونية التالية:

http://www.germanbanks.org/shOp/index.asp#verbraucherrecht;
www.deutsche-bank-pbc.pl/content/pdf/en/Internet_wniosek_umowa_ang.pdf;
https://www.firmenfinanzportal.de/fb/en/pdf/agb_GeschaeftsbedigungenFernkommunikation_en. pdf

(٤) انظر نموذج لهذه العقود على العنوان الإلكتروني التالي:

http://www.nationwide.co.uk/internetbanking/help/help_terms_n_conditions_WP6.htm

تختلف من عقد لآخر، وتشتمل على تحديد هوية العميل، والبيانات اللازمة للتعرف عليه، وجدول بالرسوم والنفقات الخاصة بالخدمة المراد الحصول عليها، ومدة العقد، وواجب السرية، والوسيلة التي ستستخدم لنقل الأوامر والطلبات بين البنك والعميل، والوسيلة التي يمكن من خلالها أن يعترض العميل على طريقة التنفيذ والمدة المسموح له فيها بذلك. أما الشروط الخاصة فهي التي تنظم علاقة البنك الإلكتروني بالعميل بصورة مفصلة بحسب طبيعة الخدمة المصرفية (إصدار نقود إلكترونية، تحويل إلكتروني للنقود....)[1].

(٤) العقود المصرفية على شبكة الإنترنت تقوم على الإعتبار الشخصي:

١٥٤- يقصد بالإعتبار الشخصي كأحد خصائص العقود المصرفية على الإنترنت ارتباط انعقاد العقد المصرفي واستمراره بتوافر مقومات الثقة في أشخاص البنك وعميله.

وتحتل الإعتبار الشخصي بالمعنى السابق أهمية أكبر لدى البنك، حيث يحرص قبل أن يعتمد التعاقد مع العميل- خاصة إذا كانت التعاقدات تنطوي على مخاطر مالية- على التأكد من توافر المقومات التي تمكنه من الحصول على أحد الخدمات المصرفية التي يقدمها، من جدارته الائتمانية، وسلوكياته الشخصية، وغيرها من العوامل التي يرى البنك ضرورة توافرها في العميل. والبنك لا يقدم على التعاقد إلا إذا اطمئن لهذه العناصر، فإذا طرأ ما يشكك فيهما تعرضت العلاقة بينهما إلى الانهيار.

١٥٥- وعلى الرغم من أن الاعتبار الشخصي بالمفهوم السابق أمر تتميز به

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 192.

العقود المصرفية منذ القدم، إلا أن هذا المفهوم قد شهد تطورا في الفترة الأخيرة؛ حيث لم يعد يقتصر على مجرد الجدارة المرتبطة بالملاءة المالية، بل أصبحت تقيم أيضا في ضوء سلوكيات العميل، ومدى مشروعية مصدر حصوله على الأموال التي يتعامل بها مع البنك، وذلك تجنبا لوقوع جرائم غسيل الأموال التي شهدت انتشارا واسعا ساعدت عليه استخدام الوسائل الإلكترونية في تنفيذ المعاملات المصرفية[1]. أيضا تطور مفهوم الاعتبار الشخصي بخصوص قرار العميل بالتعامل مع بنك إلكتروني دون آخر، حيث لم يعد يقرر ذلك في ضوء معاملات البنك السابقة، وسمعته التجارية فقط[2]، ولكن أيضا في مدى اعتماد البنك على أجهزة وبرامج ذات كفاءة عالية، ومدى مراعاته للاعتبارات الأمنية خاصة في ظل التعامل عن بعد عبر شبكة الكترونية مفتوحة على العالم بأسره كشبكة الإنترنت[3].

والاعتبار الشخصي بالمعنى السابق لا يؤثر فقط في انعقاد العقد، ولكن في بقائه أيضا. فاستمرار علاقة العميل بالبنك تتوقف على استمرار عوامل الثقة بينهما فإذا زالت هذه الثقة، أو حدث أي طارئ يؤثر عليها، كإفلاس العميل أو

---

(١) **د. محمد عبد السلام محمد**، مرجع سابق، ص ١٥٠٩.

Apostolos Ath. Gkoutzinis; Op, Cit, p189

(٢) **د. على جمال الدين عوض**، مرجع سابق، ص٣٦.

(3) (As the proportion of distant services increases, consumer loyalty becomes a more significant factor affecting changes in financial industry. It is mainly caused by the rapid development of Internet and telecommunication technologies that transforms many financial services into distance services).

Valters Kaze, Ilona, Erika Sumilo, Roberts Skapars; Op, Cit. p. 180; **Summary country report Germany**, SEB, P 8, available at: https://www.thebenche.com/reports/**germany.pdf**

إعساره أو امتناعه عن الوفاء بالتزاماته، جاز للبنك الإلكتروني وقف التعامل، وإنهاء علاقته بالعميل، دون أن يسأل البنك عن هذا الإنهاء.

أيضا بالنسبة للعميل يتوقف استمرار تعامله مع البنك على استمرار العناصر التي راعى وجودها فيه عند التعاقد. وبهذا تكون الجدارة الائتمانية شرط ابتداء وانتهاءً لعلاقة البنك الإلكتروني بالعميل(١).

١٥٦- ويترتب على أهمية الاعتبار الشخصي في العقود المصرفية على الإنترنت بالمعنى السابق بعض الآثار القانونية التي يجب أن تراعى عند إبرام هذه العقود أهمها:

(أ) ضرورة حرص البنك العامل على شبكة الإنترنت في التعاقد مع جهات للتوثيق الإلكتروني، لتتولى مهمة تعريف البنك وتبصيره بشخصية المتعاقد معه على النحو المطلوب، من حيث مدى أهليته القانونية والمالية لهذا التعاقد من عدمه.

أيضا ستقوم هذه الجهة ببث الطمأنينة لدى هذا المتعاقد من أنه فعلا يتعامل مع الموقع الحقيقي للبنك، مما سيجعله يقدم كل البيانات المطلوبة للتعاقد وهو مطمئن من أنه لا يتعامل مع موقع وهمي، أو أنه يتعامل مع بنك إلكتروني غير الذي يريد التعامل معه(٢).

(ب) يجب على البنك الإلكتروني أن يؤكد عند قيامه بالإعلان عن خدمة مصرفية ما- حتى لو كانت هذه الخدمة مصحوبة بنموذج العقد الذي يحكم

---

(١) د. عبد الرحمن قرمان، مرجع سابق، ص٩٦.

(2) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 187.

تقديمها- أن هذا لا يعد إيجابا ملزما للبنك ينعقد به العقـد بمجـرد إعـلان المتعاقد عن قبوله للخدمة بشروطها المبينة بالعقد، وإنما هذا هو مجرد دعوة للتعاقد؛ وذلك حتى لا ينخرط البنك في علاقة مصرفية إلا بعد التبيين والتحقق من شخصية المتعاقد معه، والتأكد من جدارته الائتمانية.

المبحث الثاني

قواعد إبرام العقود المصرفية على شبكة الإنترنت

بعد الوقوف على تعريف العقود المصرفية على شبكة الإنترنت، وإبراز أهم خصائصها، يحين الوقت للتعرف على القواعد القانونية التي تحكم إبرام هذه العقود.

١٥٧- ونود أن نسجل في بداية الأمر أن القواعد التي تحكم إبرام العقود المصرفية على شبكة الإنترنت لا تختلف عن القواعد الخاصة بالعقود المصرفية التي تبرم في الواقع المادي الملموس، وإن كانت تختلف معها في وسيلة إبرام هذه التعاقدات. فمثلا التراضي في التعاقدات المصرفية الإلكترونية التي تتم عبر شبكة الإنترنت يحمل ذات المضمون في التعاقدات المصرفية التقليدية، ولكن الوسيلة المستخدمة في التعبير عنه في التعاقدات الإلكترونية التي تتم عبر شبكة الإنترنت وسيلة إلكترونية، عكست بعض أوجه الخصوصية على قواعد الإيجاب والقبول في التعاقدات المصرفية الإلكترونية التي تتم عبر شبكة الإنترنت(1).

أما فيما يخص الركنين الآخرين وهما المحل والسبب، فهما ركنان ضروريان ولازمان في كل العقود المصرفية الإلكترونية التي تتم عبر شبكة الإنترنت ولكن لا يتمتعان بخصوصية معينة، حيث تطبق ذات القواعد التي تحكم

---

(1) **Apostolos Ath. Gkoutzinis** ; Op, Cit, p. 29.

- فلا جدال في أن التعاقد عبر الانترنت يخضع للقواعد العامة بشأن العقود ما لم تؤد خصوصية هذا النوع من التعاقد إلى الحاجة لبعض القواعد الخاصة د. **أسامة أبو الحسن**، مرجع سابق، ص ٦٥.

N. stephan Kinsella, Andrew F.Simpson; Op. Cit, p. 96

العقود التقليدية، فالمحل يجب أن يكون ممكنًا ومشروعًا ومعينًا، أما السبب فيجب أن يكون موجودًا ومشروعًا(1).

لذلك لا ينبغي لمن يتحدث في التعاقدات المصرفية التي تتم عبر شبكة الإنترنت أن يجهد نفسه في كتابة مطولة لكل أحكام وقواعد إبرام هذه العقود، فلن يجنى من هذا سوى فائدة محدودة؛ حيث إن هذه العقود لا تزال تخضع للقواعد العامة لإبرام العقود المصرفية، لكن ما يجب أن يسترعى اهتمامنا هو أثر استخدام شبكة الإنترنت كوسيلة إلكترونية للتعاقد عن بعد، على الطبيعة الخاصة التي تحكم إبرام العقود المصرفية، وما تتطلبه هذه العقود من اعتبارات معينة.

لذا سنعرض في مطلب أول للمرحلة السابقة على التعاقد المصرفي، وفى مطلب ثانى لقواعد الإيجاب في العقود المصرفية على شبكة الإنترنت، وفى مطلب ثالث للقواعد الخاصة بالقبول في العقود المصرفية على شبكة الإنترنت.

المطلب الأول

المرحلة السابقة على التعاقد المصرفي

عبر شبكة الإنترنت

١٥٨- تكتسب المرحلة السابقة على التعاقد المصرفي على شبكة الإنترنت أهمية خاصة، هذه الأهمية مبعثها الطبيعة الخاصة لشبكة الإنترنت، كوسيلة إلكترونية

(١) د. فايز عبد الله الكندرى، مرجع سابق، ص٥٩٩.

للاتصال عن بعد، يغيب في ظلها الحضور المادي للمتعاقدين، ذلك في ظل ما يتسم به التعاقد المصرفي من خطورة، مبعثها طبيعة المعاملات المالية والائتمانية محل هذا التعاقد، وما تحتاج إليه في ظل ذلك من أمور معينة أهمها ضرورة تعريف العميل بطبيعة الخدمة المصرفية، وكيفية التعاقد بشأنها، وما يجب أن يقدمه للبنك للحصول عليها، وما يجب أن يراعيه العميل من احتياطات لأمن التعامل المصرفي. أيضا التزام العميل بإخبار البنك بكافة البيانات التي يطلبها بصورة صحيحة ودقيقة، هذا من ناحية.

ومن ناحية أخرى البنك حريص كل الحرص على أن يتعرف على شخصية عميله من نواحي مختلفة قبل أن يتعاقد معه بشأن أحد الخدمات المصرفية التي يقدمها، وهذا الأمر يكتسب أهمية خاصة عندما يكون التعاقد في ظل عدم الحضور المادي للمتعاقدين (البنك وعميله)، بما يعكس أهمية تعرف البنك واستيثاقه من شخصية عميله. أيضا يحرص العميل على التأكد من أنه يتعامل بالفعل مع الموقع الإلكتروني للبنك، وليس مع مجرد موقع وهمي.

أيضا يثور في ظل كل ذلك التساؤل عن مدى أهمية التفاوض بين البنك والعميل حول الشروط التي تنظم تقديم البنك للخدمة المصرفية عبر شبكة الإنترنت، ومدى إمكانية إتمام ذلك عبر هذه الشبكة.

لذلك سنعرض في هذا المطلب، للالتزام بالإعلام في التعاقد المصرفي (فرع أول)، وللتوثيق الإلكتروني في التعاقد المصرفي (فرع ثاني)، مدى أهمية التفاوض في التعاقد المصرفي (فرع ثالث).

الفـــرع الأول

الالتزام بالإعلام في التعاقد المصرفي

على شبكة الإنترنت

١٥٩- يعرف الالتزام بالإعلام كواحد من أهم الالتزامات التي تقع على عـاتق الطرف الأقوى والأكثر خبرة ودراية في العقد، بإعلام وإخبار الطرف الضعيف عند التعاقد، بكافة البيانات التي تساعد الأخير على تكوين إرادة مـستنيرة إمـا بالتعاقد أو بالعدول(١).

ويجد هذا الالتزام المجال خصبًا في التجارة الإلكترونية، وذلك بالنظر إلى تواجد المستهلك في موقف ضعيف بالمقارنة بالمنتج؛ من حيث المعرفة والدراية بطبيعة السلعة أو الخدمة محل التعاقد، وكيفية التعاقد بشأنها، والاستفادة منها(٢).

---

(١) يجب ملاحظة الفارق بين الالتزام بالإعلام قبل التعاقد، والالتزام بالإعلام بعد التعاقد، حيث إن الأول يعد شرط من شروط صحة العقد، والذي يمكن المطالبة بإبطال العقـد بناء على عدم توافره، أما الثاني فهو ليس شرطا من شروط العقـد، بـل هـو مـن مقتضياته وفقا لطبيعة محله، ومن ثم فهو مفترض حتى ولو لم يـنص عليـه العقـد صراحة، وبالتالي لا يمكن المطالبة بإبطال العقد بسبب عدم النص عليه.

(2) **Rosa Julia-Barceld**, Electronic contracts, Computer law & Security report Vol. 15. no. 3 1999, p. 151.

- وقد ترجم القانون الفرنسي الخاص بحماية المستهلك ذلك في المادة ١١١، حيث نـص على التزام مقدمي السلع والخدمات عبر الانترنت بوضع وصف تفصيلي للـسلعة أو الخدمة التي يقدمونها، مشفوع بكافة البيانات الخاصة بهذه الـسلعة أو الخدمـة مـن شروط الحصول عليها، وخصائصها، وثمنها، وكيفية استلامها.

Nicole Atwill, France: adapting the french legal framework to promote electronic commerce, law library of congress, order code: LL-

ويطل علينا هذا الالتزام برأسه عند الحديث عن المرحلة السابقة على التعاقد المصرفي على شبكة الإنترنت؛ تلك المرحلة التي يظهر فيه البنك كطرف قوى؛ باعتباره القائم على تقديم الخدمة المصرفية، والأكثر قدرة على الإلمـام بكافـة الجوانب الفنية التي تحكم تقديمها عبر شبكة الإنترنت، والأكثر إحاطة بالمخاطر المحيطة بها، والقدرة على تفادى هذه المخاطر هذا من ناحية. ومن ناحية أخرى تفرض طبيعة التعاقد عن بعد عبر شبكة إلكترونية للاتصالات، بخصوص خدمة مصرفية مسئولية كبيرة على عاتق البنك، بإحاطة عميله علما بكافـة الجوانـب المتعلقة بتقديم الخدمة المصرفية.

ولاشك في أن الصورة التي يظهر عليها هذا الالتزام من قبل البنك، هـي قيام الأخير بتزويد العميل بكافة البيانات والإرشادات والنصائح التي تمكنه مـن الإلمام بتفاصيل الحصول على الخدمة المصرفية، بداية من التعرف على شروط

FLB2000.04, June 2000, p 7; **The new banking delivery system-the internet**; Op. Cit, p. 2

هذا وقد ظهرت في مجال التجارة عبر الانترنت نظم إلكترونية، تعمل علـى ترتيـب وإدارة التعاقد بين الأطراف المتعاقدة بصورة إلكترونية، بحيث تحيط هذه الأطـراف علما بالحقوق والالتزامات القانونية الواقعة على عاتق كل منهما، وتحديد المـستندات اللازمة لإتمام هذا التعاقد، بل وتعمل على إعطاء شرح قانوني لما قد يحتـاج إليـه المتعاقدان بخصوص العقد، ويتم ذلك بطريقة إلكترونية. ومـن أشـهر هـذه الـنظم (**FAS**_AFree Alongside ،(Advise system **INCAS**_INCoterms) .ShipB.)

Yao-Hua Tan - Walter Thoen, INCAS: a legal expert system for contract terms in electronic commerce, Elsevier Science B.V, (Decision Support Systems), 2000, p. 390.

www.elsevier.comrlocaterdsw; **Michael S. Baum and Henry H. Perritt**, Electronic contracting publishing, and ED1 law. Government information quarterly, Vol. 1, NO. 1. 1991, p. 104.

تقديم الخدمة، مرورا بالتعاقد عليها، وانتهاءً بالحصول عليها(١).

١٦٠-هذا ولم يعالج المشرع المصري، التزام البنك العامل عبر شبكة الإنترنت بإعلام عميله، الأمر الذي دفع بالبنك المركزي المصري وهو بصدد إصدار الضوابط الرقابية للعمليات المصرفية الإلكترونية أن يعالج هذا الأمر. فقد أوصى البنك، وهو بصدد تعامله عبر شبكة الإنترنت، أن يقوم بما يلي(٢):

- إفصاح البنك المرخص له بالقيام بالعمليات المصرفية الإلكترونية على صفحة web الخاصة به بما يفيد حصوله على ترخيص لتقديم خدماته عبر الشبكات، ورقم وتاريخ الحصول عليه، والخدمات التي يجوز للبنك تقديمها عبر شبكة الإنترنت.

- إفصاح البنك عن كون القوانين المصرية هي التي تحكم الخدمات التي يقوم بتأديتها للعملاء عبر الشبكات.

وعلى الرغم من أهمية ما قام به البنك المركزي المصري في هذا الصدد، إلا أنه لا يحقق المطلوب بالنظر إلى أهمية الالتزام بالإعلام في نظام عمل البنك العامل عبر شبكة الإنترنت، حيث إن هذه التوصيات جاءت بعبارات عامة مجملة، تفتقد إلى التفصيلات بخصوص طبيعة الخدمات التي يقدمها البنك، والخطوات الفنية للتعاقد مع البنك، والسياسة الأمنية التي تحكم التعامل مع موقعه، وغيرها من البيانات والإرشادات التي من شأنها أن تأخذ بيد العميل حتى تمام الحصول على الخدمة المصرفية عبر شبكة الإنترنت. ولاشك أن هذا

---

(1) **S.K Leong, T.Srikanthan, G.S.Hura**; Op, Cit p. 3.

(٢) **الضوابط الرقابية للعمليات المصرفية الإلكترونية وإصدار وسائل دفع للنقود** الإلكترونية، مرجع سابق، ص١٠.

الوضع منتقد، ويحتاج إلى تدخل المشرع بنصوص صريحة يلزم من خلالها البنك بهذا الأمر على النحو المطلوب.

١٦١- وعن الوضع في النظم القانونية الأخرى، فقد أكد مجلس الرقابة على المؤسسات المالية الفيدرالية الأمريكي (FFIEC) على التزام البنك العامل عبر شبكة الإنترنت بهذا الالتزام في مواجهة عملائه، بأن يوضح لهم كافة البيانات الخاصة بالخدمات التي يقدمها على الموقع الإلكتروني الخاص به(١). وقد عالج المجلس هذه البيانات، وأولى اهتماما خاصا بالإرشادات المتعلقة بالتعامل مع الموقع الإلكتروني للبنك، والتي من أهمها(٢):

---

(١) وقد ألزم مجلس الرقابة البنك أيضا بضرورة عرض هذه البيانات بصورة مكتوبة وواضحة، وأن يمكن العميل من الاحتفاظ بنسخة منها، سواء من خلال تحميلها على الكمبيوتر الخاص به أو طباعتها مباشرة. ولعل الهدف من هذا الإلزام حماية العميل باعتباره الطرف الضعيف في العملية التعاقدية، وذلك من خلال إتاحة الفرصة أمامه كاملة للاطلاع على هذه البيانات ودراستها والحصول على الاستشارة اللازمة بخصوصها من خلال عرضها بصورة مكتوبة وإمكانية الاحتفاظ بها.

Interagency council issues guidance on electronic financial services and consumer compliance; Op. Cit, p. 3-4

(2) **E-Banking,** Federal Financial Institutions Examination Council; Op. Cit, p. 14.

- قريب من هذا ما نص عليه قانون التجارة الإلكترونية التونسي رقم ٨٣ لسنة ٢٠٠٠ في الفصل (٢٥) في خصوص البيع الإلكتروني على شبكة الانترنت، حيث نص على " يجب على البائع في المعاملات التجارية الإلكترونية، أن يوفر للمستهلك بطريقة واضحة ومفهومة، قبل إبرام العقد المعلومات التالية:هوية وعنوان وهاتف البائع أو مقدم الخدمة، وصفا كاملا لمختلف مراحل انجاز المعاملة، طبيعة وخصائص وسعر المنتج، كلفة تسليم المنتج ومبلغ تأمينه والادعاءات المستوجبة، الفترة التي يكون خلالها المنتج معروضا بالأسعار المحددة، شروط الضمانات التجارية والخدمة بعد البيع، طرق وإجراءات الدفع، وعند الاقتضاء شروط القروض المقترحة، طرق وآجال التسليم وتنفيذ العقد ونتائج عدم انجاز الالتزامات. إمكانية العدول عن الشراء

١) وضع كافة البيانات الخاصة بالتعريف بالبنك وكشف هويته في مكان واضح على الموقع الإلكتروني للبنك، كعلامته التجارية ورقم تسجيله (سجل تجارى)، ورقم قيده لدى جهة الرقابة، حيث تفيد هذه البيانات في التأكد من أنه يتعامل مع الموقع الحقيقي للبنك.

٢) السياسة الأمنية التي تحكم استعمال موقع البنك والتعامل معه، وتحديد مسؤوليات العميل بخصوصها، خاصة ما تعلق منها بالمحافظة على سلامة هذه البيانات.

٣) السياسة التي تحكم الحفاظ على سرية البيانات الخاصة بالمعاملات المصرفية التي تتم عبر موقع البنك، وذلك من خلال(١):

أ- توضيح التعليمات والإرشادات التي يجب على العميل الالتزام بها أثناء التعامل مع موقع البنك، وذلك بما يتفق مع القوانين الخاصة بالسرية.

واجله، كيفية إقرار الطلبية، طرق إرجاع المنتج أو الاستبدال وإرجاع المبلغ، كلفة استعمال تقنيات الاتصالات حين يتم احتسابها عل أساس مختلف عن التعريفات الجاري بها العمل، شروط فسخ العقد إذا كان لمدة غير محدودة، والمدة الدنيا للعقد (فيما يخص العقود المتعلقة بتزويد المستهلك بمنتج أو خدمة خلال مدة طويلة أو بصفة دورية)، ويتعين توفير هذه المعلومات الكترونيا ووضعها على ذمة المستهلك للاطلاع عليها في جميع مراحل المعاملة".

(١) انظر أحد نماذج البنوك العاملة عبر شبكة الانترنت في الولايات المتحدة الأمريكية، والتي وضعت سياسة عامة تحكم الحفاظ على سرية البيانات المصرفية، من خلال أنواع البيانات المطلوب من العميل تقديمها للبنك، وسلطات البنك حيال هذه البيانات، والحالات التي يحظر عليه الكشف عن هذه البيانات فيها، والحالات التي يمكن له فيها الكشف عنها. انظر:

Bank of Internet USA, Privacy policy, January 2006, available at: http://www. bankofinternet.com/privacy-policy.aspx

ب- رسم الخطوات التي يجب على العمل اتباعها أثناء إدخال البيانات الخاصة به، وتمكينه من إخفاء هذه البيانات عن المشاركين في التعامل مع موقع البنك كمقدمى الخدمات الإلكترونية للبنك.

١٦٢- أيضا نظم البرلمان الأوربي التزام البنك العامل عبر شبكة الإنترنت بالإعلام، وذلك في التوجيه الخاص باستخدام وسائل الاتصالات الإلكترونية في التجارة الإلكترونية (٢٠٠٢/٢٠١٣)(١). وقد أولى هذا التوجيه اهتماما خاصا بالإرشادات الخاصة بكيفية التعاقد. وقد شددت هذه التوجيهات التزام البنك بعرض هذه الإرشادات بشكل واضح ومفهوم للعميل قبل أن يطلب الخدمة المصرفية، وهى(٢):

(١) الخطوات الفنية المختلفة اللازمة لإبرام العقد المصرفي عبر شبكة الإنترنت، بداية من كيفية التوصل لنموذج العقد الموجود على موقع البنك والذى يحكم تقديم الخدمة المصرفية، والكيفية التي يمكن من خلالها التعرف على بنود العقد وشروطه، والطريقة التي يمكن من خلالها للعميل أن يعبر عن إرادته للالتزام بهذا العقد.

(٢) كافة الوسائل الإلكترونية المتاحة والتي من خلالها يستطيع العميل تصحيح أي خطأ يتعلق بأى بيان من البيانات المدخلة أثناء التعاقد.

(٣) اللغات التي يمكن من خلالها إبرام العقد المصرفي.

---

(1) **Directive EU,** Electronic communications, Official Journal of the European Communities, , 2002 No. 2013, Arts (6-7-8). Available at: www.Opsi.gov.uk/ si/si2002/uksi_20022013_en.pdf

(2) **Apostolos Ath. Gkoutzinis**; Op, Cit, p.184.

(٤) بنود العقد والشروط العامة في شكل نموذجي، على نحو يسمح للعميل أن ينقل هذه الشروط ويخزنها.

(٥) الخطوات الفنية الواجب على العميل القيام بها لتأمين إرسال البيانات الخاصة بالتعاقد، ككيفية وضع الشفرة- بصورة إلكترونية- الخاصة بأى معاملة مع البنك، وأى معلومات متعلقة بهذا.

(٦) ما إذا كان نموذج العقد بعد إبرامه سيكون محفوظًا لدى البنك الإلكتروني وعلى العميل طلبه حتى يرسل إليه مثلا عبر البريد الإلكتروني، أم سيكون متاحًا على موقع البنك ويستطيع العميل الدخول عليه بكلمة مرور (password) معينة[١].

ويبدو لنا أن البنك يجب أن يجعل هذه الإرشادات معروضة بصورة واضحة ومفصلة ومصاحبة لكل عقد على حدة أي لا يجعل هذه المعلومات موحدة لكل التعاقدات، بحيث تأتى هذه الإرشادات ملائمة لنوع الخدمة المصرفية وتفصيلاتها الخاصة (حيث تختلف خطوات التعاقد باختلاف طبيعة الخدمة

---

(١) انظر نموذج لعقد مصرفي يتضمن على التعليمات والبيانات اللازمة لإبرام العقد.

Net Bank, Open an account, available at: https://Secure.netbank.com/cgi-bin/universe?LM=56

- 1.2 (The terms may be accepted on line by the following instructions set out on the relevant screen page .in addition you agree that any use by you of the internet Banking Service shall constitute your acceptance of the terms. We recommend that you store or print off a copy of the terms for your records).

HSBC, Internet banking terms and conditions, available at: http://www.bahrain.hsbc.com/public/meregional/bahrain_hom/pOpups/en/bah_pib_terms.jhtml

المصرفية)، وذلك من خلال شرح الخطوات بصورة مرتبة ومسلسلة على النحو الذي يأخذ بيد العميل حتى تمام إبرام هذا العقد، والحصول على الخدمة المطلوبة.

والسؤال: ما مدى التزام البنك بوضع هذه البيانات؟ بمعنى آخر هل يلتزم البنك بوضعها أم أنه بالخيار بين وضع هذه البيانات من عدمه؟

١٦٣- ويبدو لنا أن قيام البنك بوضع هذه البيانات هو التزام يثقل كاهله، وليس مجرد حق يملك حياله سلطة تقديرية. وهذا الالتزام لا يجد مصدره في العقد المصرفى، حيث أننا نتحدث عن التزام قبل إبرام العقد، ولكن يجد مصدره في اعتبارات حسن النية التي يجب أن تهيمن على مجريات العلاقة بين البنك وعملائه.

وتجد اعتبارات حسن النية بهذا المعنى صدى واسعًا في المعاملات التجارية؛ وذلك لارتباطها الشديد بنظرية حماية الأوضاع الظاهرة وثقة الأفراد، تلك التي تسعى التشريعات التجارية المختلفة دائما إلى التأكيد عليها وحمايتها؛ تحقيقا لسرعة واستقرار المعاملات التجارية.

ولاشك أن أولى مفردات حسن النية من قبل البنك أن يراعى الفارق بينه وبين العميل في الإلمام بالطبيعة الفنية للوسيط الإلكتروني(شبكة الإنترنت)، وما يفرضه ذلك من ضرورة تبصير العميل بالجوانب المختلفة للتعامل مع هذا الوسيط. يضاف إلى ذلك الطبيعة الخاصة للخدمة المصرفية، وما تحتويه من جوانب مختلفة (قانونية ومحاسبية واقتصادية)، تستدعى إحاطة العميل بها علما قبل التعاقد عليها، خاصة إذا ما كان التعاقد بشأنها يتم عبر شبكة إلكترونية للاتصال عن بعد.

وبناءً عليه نخلص إلى التزام البنك بإعلام العميل بكافة البيانات اللازمة للتعرف على طبيعة الخدمة المصرفية وشروط الحصول عليها، أيضا يلتزم البنك باعلامه بالبيانات اللازمة للتعامل مع الموقع الالكترونى للبنك لإبرام العقد المصرفي بصورة صحيحة وآمنة، وذلك قبل التعاقد.

بل يجب أن يحرص البنك بعد انتهاء المرحلة السابقة على التعاقد على النص صراحة على هذا الإلتزام فى العقد المصرفى الذى سينظم علاقته بالعميل، خاصة إذا كانت الخدمة المصرفية محل العقد مستمرة، وذلك على النحو الذى يجعل العميل دائما فى حاجة للاعلام بالتفاصيل التى تمكنه من الحصول على الخدمة المصرفية على أكمل وجه.

وقد أكد التوجيه الأوربي على أهمية هذا الالتزام في مواجهة البنك، وشدد على مسئوليته في هذا الخصوص(١).

والسؤال: ماذا لو أخل البنك بالتزامه بإعلام العميل، كما لو لم يقم بوضع الإرشادات اللازمة، أو وضعها بطريقة معيبة (ناقصة، غير واضحة، غير صحيحة)؟

١٦٤- الإجابة على هذا التساؤل قد توجد في النظام القانوني المصري بطريقة غير مباشرة، وذلك تحت أسم **الكتمان التدليسى**(٢)؛ والذي عبرت عن المادة ١٢٥ من القانون المدني بالقول **(يعتبر تدليسا السكوت عمدا عن واقعة أو ملابسة إذا ثبت أن المدلس عليه ما كان ليبرم العقد لو علم بتلك الواقعة أو الملابسة).**

---

(1) **Directive EU**, Electronic communications, Official Journal of the European Communities, Art (13).

(٢) **د. سعيد سعد عبد السلام**، الالتزام بالإفصاح في العقود، مرجع سابق، ص ٧٨.

وعلى الرغم من أهمية هذا الحكم، إلا أنه لا يروى ظمأنًا بخصوص التعاقد المصرفي عبر شبكة الإنترنت؛ والذي يحتاج قدرا أكبر من مسئولية البنك عن إخلاله بالالتزام بالإعلام؛ بحيث لا يقتصر الأمر عند حد السكوت العمدى، والذي يحمل معنى التدليس والخديعة، بل يجب أن يشتمل أيضا على حالة السكوت الخاطئ عن سهو أو تقصير، على أن يعطى العميل في هذه الحالة الحق في إبطال العقد للغلط. ويبرر مسئولية البنك المشددة هذه، خصوصية التعاقد المصرفي عبر شبكة الإنترنت بالمعنى السابق، والذى يحتاج من البنك مزيداً من العناية والحرص.

أما عن موقف النظم القانونية الأخرى؛ فقد عالج التوجيه الأوربي سالف الذكر هذه الحالة صراحة، حيث أكد حق للعميل الذي أبرم العقد مع البنك في ظل عدم وجود هذه الإرشادات، أو وجودها بطريقة معيبة أن يطالب بإبطال العقد(١).

ويضاف إلى إمكانية إبطال العقد من قبل العميل في حالة إخلال البنك بالتزامه بالإعلام، قيامه بالرجوع على البنك بموجب قواعد المسؤولية التقصيرية، بالنظر إلى الضرر الذي لحقه من جراء خطأ البنك.

١٦٥- وفى المقابل، يجب أن يقوم العميل بالاطلاع على كل هذه التعليمات والبيانات التي يعرضها البنك بخصوص التعاقد معه، وأن يتبع هذه التعليمات بدقة. كما يجب عليه قبل أن يلقى بنفسه في فلك أي عقد يحكم إحدى الخدمات المصرفية التي يقدمها البنك أن يقرأ بنود هذا العقد بروية، وله أن يحصل على

(1) **Directive EU,** Electronic communications, Official Journal of the European Communities, Art (15).

نسخة من هذا العقد من خلال تحميله على دعامة مادية (كمبيوتر/ اسطوانة)، أو طباعته. أيضا له أن يستشير من يريد حول الآثار القانونية الخاصة بهذا التعاقد. وهذا ما أكد عليه القضاء الأمريكي في العديد من أحكامه(١).

أيضا يلتزم العميل بالإدلاء بكافة البيانات التي يحددها له البنك عن التعاقد، واللازمة له، وأن يراعى الدقة في هذه البيانات، وأن يراعى الخطوات الموضوعة من قبل البنك لإدخال هذه البيانات.

هذا وقد عالج البنك المركزي المصري فيما صدر عنه من ضوابط رقابية مسئولية العميل عن صحة المعلومات التي يقوم بتقديمها للبنك عبر شبكة الإنترنت(٢)، لكنه لم يفصح عن الصلاحيات التي يمتلكها البنك في مواجهة العميل في حالة قيام الأخير بإدخال بيانات خاطئة.

أيضا التوجيه الأوربي سالف الذكر لم يعالج مسئولية العميل عن البيانات الخاطئة التي يقوم بإدخالها.

وعلى الرغم من هذا الصمت التشريعي عن معالجة هذا الأمر إلا أن منطق الأمور يقضى بحق البنك في أن يطلب إبطال العقد سواء للغلط أو التدليس، في حالة إذا ما أثبت عدم صحة البيانات التي قام العميل بالإدلاء بها أثناء التعاقد.

---

(1) **Laura Darden , Charles Thorpe,** Forming contracts over the internet: Click-wrap and browse-wrap agreements, Georgia state university, Law and the internet-summer 2003, p 8.

(٢) الضوابط الرقابية للعمليات المصرفية الإلكترونية وإصدار وسائل دفع للنقود الإلكترونية، مرجع سابق، ص١١.

الفرع الثاني

التزام البنك بالتحقق من شخصية العميل

عبر شبكة الإنترنت

١٦٦- يقف في مقدمة الإجراءات السابقة على إبرام العقد المصرفي بين البنك وعمليه عبر شبكة الإنترنت، قيام الأول بالتحقق من شخصية الثاني(١). وقد تحلى هذا الإجراء بثوب الخصوصية في نظام عمل البنوك العاملة على شبكة الإنترنت. وتبرر هذه الخصوصية بأمرين:

الأول: طبيعة الوسيلة التي يعتمد عليها البنك في التعاقد مع عملائه وهى شبكة الإنترنت والتي تتسم بأنها وسيلة إلكترونية للتعاقد عن بعد، الأمر الذي يظهر حاجة البنك إلى التعرف على شخصية من يتعاقد معه، والتأكد من صلاحيته لهذا التعاقد.

الثاني: الطبيعة الخاصة للعقود المصرفية، وكونها تعظم من الاعتبار الشخصي للعميل، الأمر الذي تزيد معه درجة حرص البنك على التعرف مقدما على شخصية من يتعاقد معه، خاصة بعد أن أصبح مفهوم الاعتبار الشخصي لا يقتصر على مجرد الجدارة المالية والائتمانية للحصول على إحدى الخدمات المصرفية، بل أضيف إليها بعد جديد، يتمثل في التحقق من مشروعية الأموال

---

(1) **Kit Burden**; Op. Cit, p. 248;

- د. **حسين الماحى**، نظرات قانونية في التجارة الإلكترونية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد الحادي والثلاثين، أبريل ٢٠٠٢، ص٢٩٢.

التي يتم التعامل بها مع البنك، تجنبا لوقوع جرائم غسيل الأموال، خاصة وأن فرصة هذه الجرائم ازدادت في ظل عمل هذه البنوك(1).

لهذه الاعتبارات وغيرها فرضت التجارة الإلكترونية عبر شبكة الإنترنت بصورة عامة، والبنك الإلكتروني العاملة عبر هذه الشبكة بصورة خاصة ضرورة وجود جهات وسيطة(2)، يأتي في مقدمة اختصاصاتها التعرف على شخصية المتعاقد، والتأكد من تمتعه بالأهلية القانونية التي تؤهله لإبرام العقد المصرفي، وذلك من خلال جمع المعلومات اللازمة لذلك. كما تقوم، تكملة لهذا،

---

(1) **د. محمد عبد السلام محمد**، مرجع سابق، ص ١٥٠٨.

- ويعد هذا من الالتزامات القوية التي تقع على عاتق البنك، والتي أكدت عليه العديد من الهيئات الدولية. فقد ذهبت اللجنة التنفيذية لغسيل الأموال في ١٩٨٩ إلى حث البنوك على الالتزام بهذا الأمر تحت عنوان أعرف عميلك. وقد بررت اللجنة التأكيد على هذا الالتزام بأنه يعد من الإجراءات التي يمكن الاعتماد عليها في مكافحة جرائم غسيل الأموال. أيضا أكدت لجنة بازل للرقابة على البنوك على أهمية هذا الالتزام أيضا، وذهبت إلى اعتباره حدًا أدنى من الالتزامات التي يجب أن يلتزم بها البنك للتقليل من مخاطر العمليات المصرفية. انظر :

Ross Cranston; Op. Cit, p. 134;**Interagency council issues guidance on electronic financial services and consumer compliance**; Op. Cit, p. 3.

(2) وهي شركات ناشطة في ميدان خدمات التقنية، وهي جهات تؤكد صحة التعامل على الخط، وتقدم شهادات تتضمن تأكيدا أن الطلب أو الجواب قد صدر عن الموقع المعني وتحدد تاريخ ووقت صدور الطلب أو الجواب، وحتى تتضمن شخصية المخاطب وفرت تقنيات التعريف بالشخص، بدأ بكلمة السر وانتهاء بالبصمة الصوتية، أضف إلى ذلك تقنيات التشفير. للمزيد عن دور هذه الجهات انظر العنوان التالي:

http://en.wikipedia.org/wiki/Authentication

Sofia Giannakoudi; Op. Cit, p. 220. **William Gram**; Op. Cit, p. 2; **Chris Reed**; Op, Cit, p. 36.

بإصدار شهادات موثقة تشهد بصحة التصرف ونسبته لمن صدر عنه(١).

١٦٧- ونظرا للدور المحورى الذي تلعبه جهات التوثيق فقد تصدت العديد من التشريعات الدولية والعربية لتنظيم عملها واختصاصاتها(٢). ولكن ما نود تسليط الضوء عليه في هذا الخصوص هو دور جهة التوثيق الإلكتروني في تعريف البنك الإلكتروني بعميله عبر شبكة الإنترنت، وهذا الدور من قبل جهة التوثيق يمر بخطوات معينة تهدف إلى نقل صورة واضحة للبنك عمن يتعاقد معه على أحد خدماته المصرفية عبر شبكة الإنترنت، وذلك من خلال إصدار شهادة لهذا المتعاقد لتكون بمثابة وسيلة لإثبات شخصيته أمام البنك، ومن ثم إمكانية التعاقد معه عبر موقعه الإلكتروني(٣). ويتحقق ذلك من خلال مجموعة من الخطوات وذلك على النحو التالي(٤):

---

(١) د. **سمير حامد الجمال**، مرجع سابق، ص٣٢١.

(٢) في مصر فقد نظم قانون التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة التكنولوجيا رقم ١٥ لسنة ٢٠٠٤ الأحكام المتعلقة بهيئة تنمية صناعة التكنولوجيا كهيئة توثيق إلكتروني. أيضا نظمها **التوجيه الأوربي** رقم(٩٣) لسنة ١٩٩٩ تحت مسمى مقدم خدمة التوثيق (Certification Service Provider)، أيضا قانون الصفقات الإلكترونية السنغافوري وأطلق عليها سلطة التوثيق. أيضا نظمها القانون الأمريكي في قانون التوقيع الرقمي والتوثيق الإلكتروني {Digital Signature and Electronic Authentication Law (SEAL)} الصادر في الثاني من فبراير ١٩٩٨. وقد تصدت العديد من التشريعات العربية لتنظيم هذه الجهات منها القانون التونسي رقم ٨٣ لسنة ٢٠٠٠ المتعلق بالمبادلات والتجارة الإلكترونية، وأيضا قانون المعاملات والتجارة الإلكترونية رقم (٢) لسنة ٢٠٠٢ لدولة الإمارات، وأيضا مشروع قانون المبادلات والتجارة الفلسطيني أحكام المصادقة الإلكترونية.

(٣) **محمد سعيد أحمد إسماعيل**، مرجع سابق، ص٢٠٨ وبعدها. انظر أيضا **رأفت رضوان**، مرجع سابق، ص٩٨ وما بعدها.

(4) **Alain Hiltgen. Thorsten kramp. Thomas**, Secure internet banking authentication, published by IEEE security & privacy, 2005, p.

أولا: يقوم العميل، قبل التعاقد مع البنك، بالاتصال بجهة التوثيق المتعاقد معها البنك الإلكتروني لطلب شهادة توثيق إلكتروني لمفتاحه العام الذي حصل عليه من البنك الإلكتروني (والذي يرتبط بالمفتاح الخاص للبنك الإلكتروني)، على أن يقوم العميل بتقديم الأوراق التي تثبت شخصيته (كبطاقته الشخصية، جواز السفر) والتي تطلبها جهة التوثيق.

ثانيا: تقوم جهة التوثيق بعد أن تتأكد من صحة هذه البيانات بإصدار شهادة توثيق خاصة بهذا العميل، والتي تشتمل على المفتاح العام (public key) الخاص به، والذي سيعتمد عليه البنك في التحقق من شخصية هذا العميل(١).

وتقوم جهة التوثيق قبل إصدار الشهادة بجمع المعلومات اللازمة لإصدار الشهادة سواء من طالب الشهادة مباشرة، أم من قبل الغير. ويمتنع على جهة التوثيق جمع أية معلومات غير ضرورية لإصدار الشهادة. ويحظر عليها أيضا استعمال المعلومات التي تحصل عليها خارج نطاق عملية التوثيق، ما لم تحصل من الطالب على موافقته الكتابية أو الإلكترونية(٢).

27;**Jon M. PEHA**, Electronic Commerce with verifiable audit trails, Carnegie Mellon university USA, available at:http://www.chicagofed.org/consumerinformation/what_you_should_know_about_internet_banking.cfm

- **Authentication in an Internet Banking Environment**, Federal financial institutions examination council, p 5. available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf

(1) **N. stephan Kinsella, Andrew F. Simpson**; Op, Cit, p. 18.

(٢) انظر **الفصل** (١٦) من القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية رقم ٨٣ لسنة ٢٠٠٠؛ التي تضع على عاتق جهة التوثيق أيضا التزاما بضمان صحة المعلومات الواردة في الشهادة، وذلك من تاريخ تسليم الشهادة للطالب، كما تضمن

وقبل أن تسلم جهة التوثيق هذه الشهادة للعميل تقوم بالتوقيع على هذه الشهادة بمفتاحها الخاص والذي يسمى بالمفتاح الجذري (root key)، حيث إن هذا التوقيع من شأنه إضفاء الرسمية على هذه الشهادة[1].

ثالثا: عندما يقدم العميل على التعامل مع البنك الإلكتروني فإن عليه التأكد من أن صفحة الويب الخاصة بالبنك حقيقية وشرعية، وكذلك يتأكد من أن المفتاح العام للبنك الإلكتروني لازال ساري المفعول[2]. وبعد أن يتأكد له ذلك فأن عليه أن يقوم بإرسال شهادة التوثيق الخاصة به والتي تعد بمثابة أوراق اعتماد إلكترونية (Electronic credentials) لهذا العميل[3]، هذا بالإضافة إلى كافة البيانات الخاصة بالعملية المصرفية التي يريد الحصول عليها للبنك الإلكتروني.

رابعا: قبل أن يجيب البنك طلب العميل، يقوم بالتأكد من وجود وصحة شهادة هذا العميل، وذلك من خلال الاتصال بجهة التوثيق، فإذا تم له ذلك فأنه يتابع تنفيذ العملية المطلوبة مع هذا العميل.

لاشك أن تبنى البنك الإلكتروني لنظام شهادات التوثيق المعتمدة على نظام المفتاح العام (PKI) هو من أفضل طرق التعريف بشخصية العملاء، ليس هذا فحسب، ولكن أيضا من أفضل الطرق التي يمكن للعملاء الاعتماد عليها للتأكد

أيضا الصلة بين صاحب الشهادة والتوقيع الخاص به. انظر **الفصل** (١٨) من القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية رقم ٨٣ لسنة ٢٠٠٠.، انظر أيضا المادة (٢٤) بند (١) فقرة (ب) من القانون الإماراتي رقم ٢ لسنة ٢٠٠٢ بشان المعاملات والتجارة الإلكترونية.

(1) **M. Sklira. A. S. pomportsis. M. S. Obaidat**; Op, Cit, p1780

(2) **Tips for Safe Banking Over the Internet**, Federal deposit insurance corporation, September 2000, p 1.

(3) **M.Sklira. A. S. pomportsis. M.S. Obaidat**; Op, Cit, p. 1780.

من حقيقة موقع البنك الإلكتروني على شبكة الإنترنت[1].

ونظرا للدور الكبير الذي تضطلع إليه جهة التوثيق الإلكتروني في حياة البنك الإلكتروني العامل عبر شبكة الإنترنت، والذي لا يقتصر فقط على مجرد تعريف البنك بالمتعاقد معه، بل أيضا تتضمن تقديم خدمات أمنية للبنك، فأننا بإذن الله تعالى سوف نرجئ الحديث عن التنظيم القانوني الخاص بعمل هذه الجهات من حيث أحكام التعاقد والمسؤولية للباب الثالث من هذه الدراسة.

الفرع الثالث

التفاوض في العقود المصرفية على شبكة الإنترنت

١٦٨- يعرف التفاوض بأنه " تبادل الاقتراحات، والمساومات، والمكاتبات، والتقارير، والدراسات الفنية، بل والاستشارات القانونية، فيما بين أطراف التفاوض؛ ليكون كل منهما على بينة من أفضل الأشكال القانونية التي تحقق مصلحة الأطراف، وللتعرف على ما قد يسفر عنه الاتفاق من حقوق والتزامات لطرفيه"[٢].

كما تم تعريفه بأنه "هو التحاور والمناقشة وتبادل الأفكار والآراء والمساومة بالتفاعل بين الأطراف من أجل الوصول إلى اتفاق معين حول مصلحة أو حل

(1) **Alain Hiltgen. Thorsten kramp. Thomas**; Op, Cit, p. 27.

(٢) د. **سمير حامد الجمال**، مرجع سابق، ص٩٥.

لمشكلة ما"[١].

وتبدأ المفاوضات، بدعوة يوجهها أحد أطراف التعاقد إلى الآخر، للتفاوض على إنشاء عقد مستقبلي بينهما، فيوافق الآخر على التفاوض دون ترتيب أي التزام حقيقي على كل الطرفين (إعمالا لمبدأ حرية المعاملات)[٢]. فهي لا تعتبر إيجابا ملزما بالتعاقد، كما لا يوجد أي التزام بالاستمرار في المفاوضات، ولا يترتب على العدول عنها أية مسئولية كأصل عام[٣]، أي أن المرحلة السابقة على التعاقد، تبدأ باقتراح بالدخول في مفاوضات، قد يسفر عنها إيجابا كاملا يشكل مشروعا مفصلاً ومتكاملا للعقد المراد أنشاؤه، مشتملا على العناصر الجوهرية الخاصة به، بحيث ينعقد العقد بمجرد صدور القبول[٤]، أو تسفر مرحلة المفاوضات عن اختلاف في وجهات النظر، ومن ثم عدم إبرام العقد.

١٦٩- ولا شك في أن مرحلة التفاوض هي من أهم المراحل التي يمر بها المتعاقدان، وذلك في كافة العقود بصورة عامة (التقليدية والإلكترونية). ومبعث هذه الأهمية يأتي من أنها المرحلة التي يتعرف فيها كل متعاقد على الآخر ويقدر إمكانياته، كما يتم فيها الإعداد والتحضير للعقد، وبحث كافة جوانبه الفنية والمالية

---

(١) **د. خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، المرجع السابق٢٠٩.

(2) **Avery W. Katz,** Is electronic contracting different? Contract Law in the Information Age, Travemünde conference on the economic analysis of law, 2004, p. 4. www. columbia.edu/~ak472/papers/Electronic%20Contracting.pdf

(٣) ما لم يقترن العدول بخطأ يثير المسؤولية التقصيرية، وما لم يكن هناك اتفاق خاص بشأن الدخول في مفاوضات حيث انه إذا كان هناك مثل هذا الاتفاق يمكن أن تثور المسؤولية العقدية عن الإخلال بأي التزام ورد في الاتفاق.

(٤) **بشار طلال أحمد مومني**، مشكلات التعاقد عبر الانترنت، رسالة دكتوراه كلية الحقوق - جامعة المنصورة، ٢٠٠٣م، ص٤٨.

والقانونية، وتحديد مضمونه، وتوقى المنازعات التي قد تنشأ عنه وبيان سبل تسويتها، الأمر الذي يفضى في النهاية (فى حالة استمرار المفاوضات بنجاح) إلى الإعداد الجيد لهذا العقد على ضوء مصالح ومقاصد الأطراف، ومن ثم يكتب له النجاح[1].

كما تبدو أهمية التفاوض في العقود الإلكترونية على شبكة الإنترنت بصورة خاصة من ناحيتين[2]:

الأولى: أن هذه العقود تبرم عن بعد مما يزيد من أهمية التأكد والتيقن من بعض جوانب العملية التعاقدية، مثل شخصية المتعاقد، وطبيعة المحل والضمانات وسبل التنفيذ إلى غير ذلك مما يبرز أهمية التفاوض قبل الدخول في العقد.

ثانيا: تتضمن معظم العقود الإلكترونية العديد من الجوانب الفنية الدقيقة، التي قد لا يستوعبها المتعاقد لذاته، لما تحتاج إليه من دقة وتحرى، بل والاستعانة بأهل الخبرة على نحو يعظم من أهمية التفاوض.

١٧٠- وعلى الرغم من التسليم بكل هذه الأسباب التي سيقت للتأكيد على أهمية التفاوض في العقود بصورة عامة والعقود الإلكترونية بصورة خاصة، إلا أننا لا نرى لعملية التفاوض أهمية في خصوص العقود المصرفيةِ على شبكة الإنترنت وذلك للأسباب التالية :-

١) طبيعة العمليات المصرفية وما يتعلق بتقديم خدماتها عبر شبكة الإنترنت لا تسمح بوجود مفاوضات بين البنك الإلكتروني والعميل، حيث يتمثل غالبا

(١) د. **محمد حسين منصور**، مرجع سابق، ص٥٢.
(٢) المرجع السابق، ص٥٣.

أسلوب تقديم الخدمة في قيام البنك بعرض خدماته على الموقع الخاص بـه على أن يلحق بكل خدمة نموذج العقد المتعلق بها والذى يتضمن كل شروط التعاقد وبنوده (العقود النموذجية type contract)، على نحو لا يجعل أمام العميل سوى أحد أمرين، إما أن يقبل العقد كله أو يرفضه كلـه (-Take- it or-leave-it). فالخدمات البنكية عادة ما ينفرد البنك بوضع شروط التعاقـد الخاصة بها، ويجعله متاحًا على موقعه على شبكة الإنترنت، وعلى العميـل إذا ما أراد الحصول على هذه الخدمة المصرفية أن يقوم بالاطلاع على هذه الشروط- والتي أعدها البنك سلفا- فإذا وافق على الحصول على هذه الخدمة بهذه الشروط قام بالضغط على الأيقونة التي تفيد موافقته علـى العقـد (I agree, I accept)، أو لا يوافق على شروط العقد فيرفضه جملة ومن ثم لا يتم إبرام العقد(١).

٢) أن الهدف الرئيس لإنشاء بنوك إلكترونية تعمل وتؤدى خدماتها عبر شـبكة الإنترنت هو التيسير على العملاء من خلال تقديم خدمات مصرفية لهم أينما كانوا، وعلى نحو سريع وبسيط يواكب الإيقاع الـسريع لطبيعـة التجـارة الإلكترونية على شبكة الإنترنت عامة، والبنك الإلكتروني العامل على هـذه الشبكة بصورة خاصة، الأمر الذي يدفع بالبنك إلى التخلي إلى حد بعيد عن الدخول في مفاوضات مطولة مع طالب الخدمة.

٣) أنه على الرغم من الأهمية البالغة لعملية التفاوض في العقود الإلكترونية إلا

(1) **Michael Chissick, Alistair Kelman**; Op, Cit, p. 99; **Laura Darden, Charles Thorpe**; Op, Cit, p. 5.

أن هذا لا يظهر كما ذهب بعض الفقه[1] إلا بالنسبة للعقود المركبة[2]، تلك التي أسفرت عنها الأساليب الحديثة في التعامل، حيث تتسم هذه العقود بأنها تنطوي على مجموعة من العمليات المركبة والمعقدة فنيا وقانونيا، كما أنه تنطوي على قيمة اقتصادية ومخاطر جسيمة بالنسبة لأطرافها، لذلك تظهر أهمية التفاوض هنا، وذلك على عكس العقود المصرفية عبر شبكة الإنترنت التي لا يظهر فيها مثل هذه الأمور.

هذا وقد غاب عن النظام القانوني المصري نص يراعى الطبيعة الخاصة للعقود المصرفية على شبكة الإنترنت فيما يتعلق بعملية التفاوض بين البنك وعميله.

أما عن موقف النظم الأخرى في هذا الصدد، فالملاحظ أن المشرع الألماني قد فطن للطبيعة الخاصة للبنوك العاملة عبر شبكة الإنترنت والعقود التي تبرمها هذه البنوك لتقديم خدماتها، وذلك بالنظر إلى الهدف من اعتلاء هذه البنوك لشبكة الإنترنت لتقديم هذه الخدمات، وبالنظر أيضا إلى غياب مرحلة التفاوض، فوضع

---

(١) **د. محمد حسين منصور**، مرجع سابق، ص٥٢.

(٢) **والعقود المركبة** (Contracts Complexes)هي عبارة عن عقد واحد يتكون من عدة عقود تترابط فيما بينها لتحقيق عملية واحدة. وقد كان ظهور هذا النوع من العقود نتيجة لما يكتنف المعاملات الدولية والمحلية من تركيب وتعقيد، مما تظهر معه الحاجة إلى دراسة هذا النوع من العقود من الجوانب الاقتصادية والقانونية والتقنية. ولعل من أهم صور هذه العقود المركبة في الوقت الحالي عقود التنمية الاقتصادية، وعقود التكامل في المجالات الزراعية، وعقود البوت (BOT) Build Operate Transfer، وعقود تسليم مفتاح، وعقود التأجير التمويلي Credit – Bail، وعقود الامتياز التجاري، وعقود نقل التكنولوجيا، وعقود التنقيب عن البترول، وعقود المعلوماتية. انظر في ذلك **د. خالد ممدوح إبراهيم**. إبرام العقد الالكتروني، المرجع السابق، ص٢٠٤.

لذلك قواعد خاصة بهذه العقود، تهدف في المقام الأول إلى حماية المستهلك الإلكتروني في عقود الخدمات المصرفية على شبكة الإنترنت. وقد ظهر ذلك من خلال إلزامه البنك الإلكتروني بصياغة هذه الشروط بطريقة واضحة وبسيطة وعرضها على الموقع الإلكتروني للبنك على شبكة الإنترنت، أو إرسالها عبر البريد الإلكتروني. كما ألزم البنك الإلكتروني بجعل هذه العقود مجهزة من الناحية الفنية بحيث يستطيع العميل الاطلاع على كل محتوى العقد بتحريك العقد إلى أسفل وإلى أعلى، وكذلك وضع أيقونة معينة فى نهاية العقد، بحيث بالضغط عليها تتم الموافقة(١).

١٧١- وعلى الرغم من تسليمنا بعدم أهمية التفاوض في العقود المصرفية على شبكة الإنترنت، إلا أن هذا لا يعنى عدم وجود نوع من الحوار بين البنك الإلكتروني وعميله. والدليل على ذلك أن وسائل التعاقد الإلكتروني التي يمكن للبنك أن يعتمد عليها غير مقصورة فقط على العقود النموذجية (وإن كانت هي الغالب الأعم)، حيث يمكن التعاقد من خلال التواصل السمعي والبصري الفورى (chat) مثل كاميرا الويب (Web Camera)، والميكروفون (Microphone)، أو من خلال رسائل البريد الإلكتروني (an electronic mail message)(٢)، فكل هذه الوسائل تتيح تبادل الآراء والمقترحات فيما بين البنك وعملائه بخصوص منح العميل بعض التسهيلات الائتمانية أو ما شابه ذلك، وهى أمور تختلف بحسب طبيعة علاقة البنك بالعميل ونوع الخدمة المصرفية المطلوبة.

١٧٢- ومما نود الإشارة إليه أن اتباع البنك لأسلوب التعاقد بالعقود النموذجية

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 193.

(2) **N. stephan Kinsella, Andrew F. Simpson**; Op, Cit , p. 29.

مبعثه ليس فقط طبيعة الوسيلة المستخدمة في التعاقد وهى شبكة الإنترنت، وما يترتب عليها من غياب الحضور المادي للمتعاقدين، ولكن مبعثه طبيعة العمليات المصرفية بصورة عامة، وما تحتاج إليه هذه العمليات من سرعة وسهولة في إبرام عقودها، يضاف إلى ذلك أن البنك يصيغ شروط هذه العقود ولا يقبل بخصوصها مناقشة من العميل، فإما أن يقبل العقد بحالته هذه أو يرفضه بذات حالته. والدليل على ذلك أن التعاقد بالعقود النموذجية هو الأسلوب المتبع أيضا من قبل البنوك التقليدية. لكن خصوصية التعاقد بالعقود النموذجية من قبل البنك الإلكتروني تتمثل في أمرين:

الأول: هو ضرورة وضع كافة البيانات التوضيحية للعميل، والتي تكون له بمثابة علامات مضيئة على طريق إبرام العقد المصرفي تهديه وترشده إلى الخطوات الصحيحة حتى تمام إبرام هذا العقد.

الثاني: ضرورة إلحاق كل بنود العقد بشرح وافٍ ومفصل(١)، دون أن يقتصر الأمر على مجرد سرد حرفى لهذه البنود، وذلك على النحو الذي يجعل المتعاقد على بينة بكل التزاماته ومسؤولياته، دون أن يكون في حاجة إلى من يشرح له أيا من هذه البنود.

١٧٣- وفى ظل التسليم بأن الأسلوب المتبع غالبا من قبل البنك الإلكتروني للتعاقد عبر شبكة الإنترنت هو العقود النموذجية، فإن تساؤلا يلقى بظلاله علينا، وهو: هل تعد العقود المصرفية على شبكة الإنترنت من قبيل عقود الإذعان ؟

---

(1) **Michael Chissick, Alistair Kelman**, Op. Cit, p. 100; **Apostolos Ath. Gkoutzinis**; Op, Cit, p193.

ذهب جانب من الفقه[1] إلى القول بأن هذه العقود تعتبر من قبيل عقود الإذعان، وقد ساق لتبرير ذلك عدة تبريرات، وهى:

أ- تعذر مناقشة الشروط الجوهرية في هذه العقود.

ب-تشابه هذه العقود من بنك لآخر.

ج- يضاف إلى ذلك أن التعامل مع البنوك أصبح لا غنى عنه في الحياة الحديثة.

١٧٤- لكننا لا نتفق مع هذا الرأي، ونرى أن اتسام العقود المصرفية على شبكة الإنترنت بأنها عقود نموذجية وما ترتب على ذلك من غياب عنصر التفاوض في هذه العقود، ليس من شأنه جعل هذه العقود عقود الإذعان[2] وذلك للأسباب التالية:

أ- غياب المفهوم القانوني للإذعان في هذه العقود على نحو ما قررته محكمة النقض المصرية في هذا الخصوص[3]، حيث ذهبت هذه المحكمة إلى أن "من خصائص عقود الإذعان أنها تتعلق بسلع أو مرافق تعتبر من الضرورات بالنسبة إلى المستهلكين أو المنتفعين، ويكون فيها احتكار الموجب لهذه السلع احتكارا قانونيًا أو فعليا أو تكون سيطرته عليها من شأنها أن تجعل المنافسة محدودة النطاق، وأن يكون صدور الإيجاب منه إلى الناس كافة وبشروط

---

(١) انظر هذه الآراء د. **على جمال الدين عوض**، مرجع سابق، ص ٣٨.

(٢) قريب من هذا الرأى انظر:

Ross Cranston; Op, Cit, p. 151.

(٣) **نقض مدنى مصرى**، ١٢ / ٣/ ١٩٧٤، طعن رقم ٣٩٦، س ق ٣٧، قاعدة (٨٠)، مجموعة أحكام النقض، س ٢٥، ص ٤٩٣.

واحدة ولمدة غير محدودة. والسلع الضرورية هي التي لا غنى عنها، والتي لا تستقيم مصالحهم بدونها بحيث يكونون في وضع يضطرهم إلى التعاقد بشأنها، ولا يمكنهم رفض الشروط التي يضعها الموجب ولو كانت جائزة وشديدة، كما أن انفراد الموجب بإنتاج سلعة ما لا يعد احتكارا يترتب عليه اعتبار العقد المبرم بشأنها من عقود الإذعان ما لم تكن تلك السلعة من الضرورات الأولية للجمهور بالمعنى المتقدم ".

وفي ضوء هذا المفهوم الذي أرسته محكمة النقض في خصوص تحديد مفهوم الاحتكار في عقد الإذعان، فأنه يمكن القول بأن هذا المعنى للاحتكار لا يتحقق في عقود الخدمات المصرفية عبر شبكة الإنترنت، حيث أنه على الرغم من التسليم بأن الخدمات المصرفية تعد من الضرورات التي لا غنى عنها للكافة (تجار وغير تجار)، إلا أنه لا يوجد سيطرة على تقديم هذه الخدمات من قبل بنك واحد، حيث تتعدد البنوك وتتعدد خدماتها المصرفية، على النحو الذي لا يقبل معه القول بوجود نوع من السيطرة أو الهيمنة من قبل بنك معين.

يضاف إلى ذلك أن دخول شبكة الإنترنت نطاق المعاملات التجارية أسفر عن وجود بعض الهيئات والمؤسسات التي تقدم بعض أشكال العمليات المصرفية (كإصدار النقود الإلكترونية) (١)، التي كان يفترض أنها مقصورة على البنوك وحدها، الأمر الذي ينفي تماما وجود نوع من الانفراد أو السيطرة على تقديم الخدمات المصرفية الإلكترونية عبر شبكة الإنترنت، الأمر الذي يوسع من فرصة اختيار الجهة التي يتم الحصول منها على الخدمات المصرفية ومن ثم

---

(١) د. شريف محمد غنام، المرجع السابق، ص ٨٢؛

Tahir Masood Qureshi, Op. Cit, p. 5

الوصول إلى أفضل خدمة.

ب-لا يمكن القول في ظل تعدد البنوك والمؤسسات المقدمة للخدمات المصرفية على النحو السابق أن كل البنوك سوف تتبنى صيغة موحدة لشروط عقود خدماتها المصرفية. بل أن القول الصحيح الذي يستقيم مع هذا الوضع هو احتراف البنوك في وضع شروط مخففة وتسهيلات ائتمانية وأقل مقدار للعمولة، بحيث تعمل على جذب أكبر عدد من العملاء، وذلك في ظل بيئة مشتعلة بالمنافسة(١). وهذا ما حدث بالفعل في المملكة المتحدة، فعلى الرغم من أن البنوك الإلكترونية العاملة عبر شبكة الإنترنت تتعامل مع عملائها بأسلوب التعاقد النموذجي، إلا أن صيغ هذه العقود مختلفة من بنك لأخر ولا توجد شروط موحدة تحكم هذه العقود(٢).

ج-يضاف إلى ذلك أن وضع العقود المصرفية على شبكة الإنترنت في صورة عقود نموذجية لم يكن غاية في حد ذاته، ولكنها وسيلة ملاءمة لطبيعة التعامل على شبكة الإنترنت بصورة عامة، والعقود المصرفية بصورة خاصة، والتي تحتاج لمزيد من السرعة في إبرامها وتنفيذها.

وبناءً عليه لا يمكن إطلاق القول باعتبار العقود المصرفية على شبكة الإنترنت من قبيل عقود الإذعان لمجرد أنها تظهر في صورة عقود نموذجية. بل القول الأدق في هذا الخصوص هو أن العبرة بالمعاني وليس بالأشكال والمباني، الأمر الذي يجب معه تحليل العقد في ضوء بنوده وليس في ضوء الإطار المنصب فيه، وذلك للنظر فيما إذا كان هناك إجحاف واضح بحقوق العميل على

---

(1) **Jennifer Iser**; Op, Cit, p. 1.

(2) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 192.

النحو الذي يمكن معه القول بوجود إذعان من عدمه.

وعلى أية حال إذا لوحظ هذا الإذعان من قبل العميل فله أن يحتمي بالقضاء لتطبيق المادة ١٤٩ من القانون المدني المصري والتي تقضي بأنه إذا تضمن العقد شروطا تعسفية جاز للقاضي أن يعدل هذه الشروط أو يقرر الإعفاء منها، وذلك وفقا ما تقضي به قواعد العدالة، ويقع باطلا كل اتفاق على خلاف ذلك.

وقد نظم القانون التجاري الموحد الأمريكي (UCC) أيضا سلطة المحكمة في استبعاد أي بند أو شرط يرد في العقد تراه غير ملائم أو مناسب، أو حتى الحد من آثاره في العلاقة بين المتعاقدين(١).

المطلب الثاني

الإيجاب في العقود المصرفية على شبكة الإنترنت

١٧٥- يعرف الإيجاب وفقا للقواعد العامة بأنه "التعبير البات (غير المعلق على شرط) عن إرادة شخص يعرض على آخر أن يتعاقد معه، وقد يكون موجها

---

(1) (If the court as a matter of law finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract with out the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result).; **Uniform Commercial Code**, 1997, (part3) general obligation and construction of contract.

لشخص معين كما قد يكون موجها لشخص غير معين أي موجها للجمهور[1].

ويتضح من خلال هذا التعريف أن الإيجاب يتسم بمجموعة من الخصائص هي[2]:

١)- الإيجاب عرض بات: ويعنى ذلك انصراف نية الموجب على نحو جازم بإبرام عقد معين، فإذا لم تتوافر هذه النية فلا يوجد إيجاب.

٢)- الإيجاب عرض كامل: أي يجب أن يتضمن الإيجاب العناصر الأساسية للعقد المراد إبرامه، ولا يلزم أن يتضمن المسائل التفصيلية للعقد.

٣)- الاتصال بعلم الموجه إليه: الإيجاب يجب أن يتصل بعلم الموجه إليه (الطرف الذي نشأ الإيجاب من أجله) على نحو يجعله يحاط به علما[3].

وإذا كان هذا هو مفهوم الإيجاب الذي يجرى عليه التعاقد في العقود المصرفية التقليدية، فهل ظل محتفظا بهذا المفهوم في العقود المصرفية التي تبرم عبر شبكة الإنترنت؟

---

(١) د. **فتحي عبد الرحيم عبد الله**، مرجع سابق، ص٦٨.
- عرف كذلك بأنه عرض جازم وكامل للتعاقد وفقا لشروط معينة يوجهه شخص إلى شخص آخر معين أو إلى أشخاص غير معينين أو للكافة. د. **فريد عبد المعز فرج**، مرجع سابق، ص٥٢٧.
- وقد عرفته محكمة النقض، المصرية بأنه العرض الذي يعبر الشخص الصادر منه على وجه جازم عن إرادته في إبرام عقد معين، بحيث إذا أقترن بقبول مطابق انعقد العقد. راجع نقض مدني مصري، ١٩٦٩/٦/١٩، طعن رقم ٣٢٣، س ق ٣٥، القاعدة (١٥٩)، مجموعة أحكام النقض (الجزء الأول)، س ٢٠، فقرة ج، ص ١٠١٧.

(٢) د. **أحمد شوقى عبد الرحمن**، مرجع سابق، ص ٣٧؛ د. **محمد سعيد أحمد إسماعيل**، مرجع سابق، ص١٣٠.

(3)**Roger Gerleroy Miler – Gaylord A. Jentz**; Op. Cit, p. 148.

١٧٦- لم يضع لنا المشرع المصري نصا صريحا يفيد إمكانية التعبير عن الإيجاب باستخدام الوسائل الإلكترونية. ومع ذلك يمكن أن تستشف إرادة المشرع الضمنية في تقرير إمكانية التعبير عن الإيجاب باستخدام الوسائل الإلكترونية، من خلال ما قررته المادة (١٥) من قانون التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات[١]، حيث نص على أن "للكتابة الإلكترونية وللمحررات الإلكترونية، في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة في المحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية، متى استوفت الشروط المنصوص عليها في هذا القانون وفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون".

فالمشرع المصري وفقا لهذا النص قد أسبغ ذات الحجية المقررة للكتابة التقليدية على الكتابة الإلكترونية في مجال الإثبات، ومن ثم يمكن أن يستفاد من ذلك بصورة ضمنية إمكانية استخدام رسائل البيانات الإلكترونية على شبكة الإنترنت في التعبير عن الإيجاب. يضاف إلى ذلك أنه وفقا للتعريف السابق للإيجاب، وعناصره، لا يوجد ما يحول دون إمكانية التعبير عن الإيجاب بالوسائل الإلكترونية، مادام هناك عرض بات، مشتمل على العناصر الرئيسة للعقد، ومتصل بعلم من وجه إليه.

لكن هذا الأمر يجب أن يتم تداركه من المشرع المصري، بالنص الصريح على إمكانية استخدام الوسائل الإلكترونية في التعبير عن الإيجاب.

أما على صعيد النظم القانونية الأخرى، فالملاحظ أن العديد من القوانين

---

(١) القانون رقم ١٥ لسنة ٢٠٠٤. انظر الجريدة الرسمية العدد١٧، تابع (د)، ٢٢ أبريل ٢٠٠٤.

الدولية والوطنية قد استقرت على إمكانية التعبير عن الإيجاب من خلال شبكة الإنترنت. وقد كان في مقدمة هذه القوانين القانون النموذجي للتجارة الإلكترونية الصادر عن لجنة القانون التجاري الدولي التابعة لمنظمة الأمم المتحدة(١٩٩٦) في المادة ١٢ منه حيث جاء فيه أنه "في العلاقة بين منشئ رسالة البيانات والمرسل إليه، لا يفقد التعبير عن الإرادة أو غيره من أوجه التعبير مفعوله القانوني أو صحته أو قابليته للتنفيذ لمجرد أن في شكل رسالة بيانات".

وقد سار البرلمان الأوربي على نهج لجنة القانون التجاري الدولي في هذا الخصوص حيث حظر على الدول الأعضاء وضع أي عقبة في سبيل إمكانية التعبير عن الإيجاب من خلال شبكة الإنترنت(١).

أيضا على صعيد التشريعات العربية فقد تبنت العديد منها ذات المسلك(٢). فقد نص القانون التونسي رقم ٨٣ لسنة ٢٠٠٠ الخاص بالمبادلات والتجارة الإلكترونية في الفصل الأول منه على أن "يجري على العقود الإلكترونية نظام العقود الكتابية من حيث التعبير عن الإرادة ومفعولها القانوني وصحتها وقابليتها للتنفيذ فيما لا يتعارض وأحكام هذا القانون".

نخلص مما سبق أن السواد الأعظم من التشريعات القانونية قد استقرت على

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 185.

(٢) نص القانون الإماراتي رقم (٢) لسنة ٢٠٠٢ بشأن المعاملات والتجارة الإلكترونية في المادة (١٣) (١) لأغراض التعاقد يجوز التعبير عن الإيجاب والقبول جزئيا أو كليا بواسطة المراسلة الإلكترونية. نص قانون التجارة الإلكتروني البحريني في المادة (١٠) على " إبرام العقود في سياق إبرام العقود يجوز التعبير، كليا أو جزئيا، عن الإيجاب والقبول وكافة الأمور المتعلقة بإبرام العقد والعمل بموجبه، بما في ذلك أي تعديل أو عدول أو إبطال للايجاب أو القبول، عن طريق السجلات الإلكترونية ما لم يتفق الطرفان على غير ذلك".

إمكانية التعبير عن الإيجاب بالوسائل الإلكترونية (ومنها شبكة الإنترنت) في العقود الإلكترونية. ولما كان العقد المصرفي على شبكة الإنترنت ينتمي إلى طائفة العقود الإلكترونية، فإنه يأخذ حكمها فيما يتعلق بإمكانية التعبير عن الإيجاب فيه باستخدام شبكة الإنترنت(١).

١٧٧- أما عن مفهوم الإيجاب في العقد المصرفي عبر شبكة الإنترنت، فلم يظهر لنا تعريف خاص بهذا الإيجاب؛ وذلك على اعتبار أنه لا يختلف عن الإيجاب الإلكتروني بصورة عامة.

هذا وقد عرف الإيجاب الإلكتروني بأنه عبارة عن "تعبير جازم عن الإرادة، يتم عن بعد عبر تقنيات الاتصال- سواء كانت مسموعة أم مرئية أم كلتيهما- ويتضمن كافة الشروط والعناصر الأساسية للعقد المراد إبرامه، بحيث ينعقد به العقد إذا ما تلاقى معه القبول"(٢).

كما عرف الإيجاب على شبكة الإنترنت بأنه "تعبير عن إرادة الراغب في التعاقد عن بعد، من خلال شبكة دولية للاتصالات بوسيلة مسموعة مرئية، يتضمن كل العناصر اللازمة لإبرام العقد بحيث يستطيع من وجه إليه أن يقبل التعاقد مباشرة"(٣).

وبناءً عليه، يمكن أن يعرف الإيجاب في العقد المصرفي على شبكة الإنترنت بأنه عرض بات بإبرام عقد مصرفي باستخدام شبكة الإنترنت على أن يتضمن العناصر الأساسية للعقد بحيث يتم العقد باقتران القبول به.

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 188.

(٢) **د. خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، المرجع السابق، ص ٥٢.

(٣) **د. محمد حسين منصور**، مرجع سابق، ص٦٧.

ويتضح من هذا التعريف أن الإيجاب في العقد المصرفي على شبكة الإنترنت لا يختلف عن مضمون الإيجاب في العقود المصرفية التقليدية، وأن الاختلاف فقط في طبيعة الوسيلة المستخدمة للتعبير عنه، وهى شبكة الإنترنت.

خصوصية الإيجاب في العقد المصرفي على شبكة الإنترنت:

١٧٨- على الرغم من التسليم بأن العقد المصرفي على شبكة الإنترنت ينتمي إلى العقود الإلكترونية على شبكة الإنترنت، وأن مضمون الإيجاب في كل منهما واحد، إلا أن خصوصية المعاملات المصرفية على شبكة الإنترنت، قد تعكس بعض أوجه من الخصوصية فيما يصدر عن البنك بخصوص التعاقد على أحد الخدمات المصرفية التي يقدمها، وذلك على النحو التالي:

(أولا) العميل في العقد المصرفي على شبكة الإنترنت هو الموجب:

١٧٩- سبق أن ذكرنا في تعريف الإيجاب وبيان خصائصه بأنه لابد أن ينطوي على عرض بات وجازم؛ بمعنى أنه يجب أن تتجه نية الموجب بصورة صريحة وقاطعة إلى إبرام العقد من خلال هذا الإيجاب، على نحو يمكن القول معه أنه إذا صدر من الموجه إليه الإيجاب قبول مطابق لهذا الإيجاب أنعقد العقد في الحال.

ويجرى العمل على شبكة الإنترنت غالبا في قيام منتج السلعة أو الخدمة بالتعبير عن الإيجاب، بحيث إذا ما صدر قبول من المستهلك أنعقد العقد[1].

(١) ويظهر ذلك جليا في السلع والخدمات التي يقوم أصحابها بالتعاقد عليها من خلال عقود (Click Wrap contract)، حيث يقوم صاحب السلعة أو الخدمة بعرض سلعته أو خدمته مرفقا بها العقد الذي يحكم الحصول عليها، حيث يعد ذلك إيجابا منه، وبمجرد قبول المستهلك لشروط العقد، يقوم بالضغط على الأيقونة المعدة لذلك، فينعقد العقد. ومن أشهر المعاملات التي تتم بهذا الأسلوب ترخيص البرمجيات.

لكن بالنظر إلى أهمية الاعتبار الشخصي للعميل في العقد المصرفي، خاصة في ظل التعاقد عبر شبكة إلكترونية للاتصال عن بعد، فإن ما يصدر عن البنك ليس إيجابا ملزما ينعقد به العقد بمجرد صدور قبول مطابق من العميل، بل هو مجرد دعوة للتعاقد (Invitation to treat)، يملك البنك الرجوع فيها، إذا تبين له عدم توافر الجدارة الائتمانية للعميل، أو عدم مشروعية الأموال التي يريد التعامل مع البنك بها[1].

ويحتفظ البنك بهذا الحق (ما يصدر عنه مجرد دعوة للتعاقد)، سواء كان العرض الصادر عنه خاص أم عام.

ففى حالة العرض الخاص، وذلك كما لو قام البنك بإرسال رسالة بريد إلكتروني للعميل يعرض عليه التعاقد بشأن أحد الخدمات المصرفية التي يقدمها، في هذه الحالة يتم علم العميل بهذا العرض عند فتحه لصندوق بريده الإلكتروني، فإذا وافق العميل على عرض البنك، فإن هذا لا يعد قبولا منه ينعقد به العقد[2]، لأن ما صدر عن البنك في هذه الحالة لم يكن إيجابا، بل هو دعوة للتعاقد، هذا على الرغم من أن البنك قد قام بإرسال العرض إلى عميله الذي يفترض أنه على دراية بشخصيته؛ إلا أن احتمالات عدم يسار العميل أثناء توجيه الرسالة إليه

Heather H. Bruser, Form contracts in an online world: The enforceability of click-wrap and browse-wrap agreements, The federal lawyer, October 2008, p 14.

(1) **Michael Chissick, Alistair Kelman**;Op.Cit,p. 82; **N. stephan Kinsella, Andrew F.Simpson**; Op, Cit, p. 162; **Harry SK Tan**, Electronic transactions regulation – Singapore, Computer law & Security report Vol. 18 no. 5, 2002, 345.

(٢) **د. فريد عبد المعز فرج**، مرجع سابق، ص٥٣٠.

قائمة؛ (كأن يكون العميل معرض لشهر إفلاسه ولا يعلم البنك)، الأمر الذي يعطى للبنك الحق في أن يحتفظ بحقه، في اعتبار ما يصدر عنه مجرد دعوة للتعاقد.

أما في حالة العرض العام، كما لو وجه البنك عرضه للكافة من خلال الموقع الإلكتروني له على شبكة الإنترنت، فأن حرص البنك في اعتبار ما يصدر عنه مجرد دعوة للتعاقد سوف يزداد إلى حد بعيد في هذه الحالة، حيث يجهل البنك تماما شخصية العميل(١)، ومن ثم يحتفظ بحقه في اعتبار ما يصدر عنه هو مجرد دعوة للتعاقد.

ويجب في سبيل وصول البنك لغايته هذه، أن يكون على حرص ووعي كافيين بأسلوب عرضه لخدماته المصرفية، سواء عبر موقعه الإلكتروني أم من خلال البريد الإلكتروني أو غيرها من الطرق؛ وذلك بأن يوضح جليا أن هذا العرض على الرغم من اشتماله على كافة عناصر التعاقد من المواصفات الخاصة بهذه الخدمة، ونموذج العقد المصرفي الذي سيحكم تقديمها، إلا أن هذا لا يعدو أن يكون مجرد دعوة للتعاقد، لا ينعقد العقد المصرفي بمجرد صدور قبول ممن يريد الحصول على هذه الخدمة. كما يجب على البنك أن يستخدم بعض العبارات الدالة على ذلك مثل: (دون التزام) أو (بعد التأكيد)(٢).

بل يحتاج الأمر إلى صدور إيجاب منه لهذا العرض، على أن ينظر البنك

---

(١) المرجع السابق، ص٥٣٠.

(٢) د. **أسامة أبو الحسن**، مرجع سابق، ص٧٢؛ د. **محمد حسين منصور**، مرجع سابق، ص ٦٨؛

Michael Chissick, Alistair Kelman; Op. Cit, p89

بعد ذلك في جدوى هذا الإيجاب، ويقرر بعده ما إذا كان سيقبل إبرام العقد أم لا.

وترتيبا على ما سبق ذكره، نخلص إلى أن ما يصدر عن البنك هو مجرد دعوة للتعاقد لا تلزم البنك بالتعاقد، وأن هذه الدعوة تحتاج لإيجاب من قبل العميل، على أن ينظر البنك في هذا الإيجاب ليقرر ما إذا كان سيقبله، أم يرفضه.

والسؤال الذي يطل علينا: ما هو الأسلوب الذي سيتبعه المتعاقد مع البنك للتعبير عن إيجابه بإبرام العقد؟

١٨٠- بصورة عامة يمكن القول إن التعبير عن الإيجاب عبر شبكة الإنترنت يتوقف على الأسلوب المتبع للتعاقد عبر هذه الشبكة، فإذا كان التعاقد يتم من خلال غرف المحادثة (Chatting Room) فأن التعبير عن الإيجاب يمكن أن يتم من خلال العبارة وذلك لأن هذا الأسلوب في التعاقد يسمح بالاتصال السمعي والبصري بصورة فورية للمتعاقدين، وذلك على النحو الذي يمكن فيه لكل منهما أن يعبر عن إرادته بالعبارة، أما إذا كان التعاقد سيتم من خلال البريد الإلكتروني، فأن التعبير عن الإيجاب يتم من خلال الكتابة، وذلك من خلال تبادل الرسائل الإلكترونية فيما بين المتعاقدين(١).

لكن ترتيبا على ما سبق ذكره بخصوص الطريقة المتبعة غالبا من قبل البنك الإلكتروني في التعاقد عبر شبكة الإنترنت والتي تتمثل غالبا في العقود النموذجية، فأن الأسلوب الذي سيتبع لتعبير المتعاقد مع البنك عن رغبته في التعاقد سوف يتمثل في قيام هذا المتعاقد بالضغط على الأيقونة المعدة لهذا

---

(1) **Ibid**, p. 85.

الغرض في العقد المصرفي المتاح على الموقع الإلكتروني للبنك. ويعد هذا الأسلوب للتعبير عن الإرادة من أفضل الأساليب ملاءمة لطبيعة العقود المصرفية على شبكة الإنترنت. ويعود ذلك إلى غياب التفاوض بين البنك الإلكتروني ومن يتعاقد معه، الأمر الذي لا يظهر الحاجة إلى التعاقد من خلال غرف المحادثة أو البريد الإلكتروني، ومن ثم لن يكون أمام هذا المتعاقد إلا أن يقبل العقد كله أو يرفضه كله، ومن ثم يكون التعبير عن الإرادة من خلال النقر أو الضغط على الأيقونة المعدة لذلك في العقد المصرفي أكثر ملاءمة وفاعلية(١).

وقد وجه نقدا لهذا الأسلوب تمثل في احتمالية الضغط على سبيل الخطأ أو السهو من قبل المتعاقد على هذه الأيقونة، على الرغم من أنه عزف عن التعاقد بعد الاطلاع على بنود العقد(٢).

لكن هذا النقد مردود عليه بأن البنك الإلكتروني يستطيع تفادى حدوث ذلك من خلال وضع الأيقونة الخاصة بالموافقة في نهاية العقد، بحيث لا يصل إليها المتعاقد إلا بعد أن يكون قد قام بملء كافة البيانات الخاصة بهذا العقد، يضاف إلى ذلك قيام البنك بتكرار طلب الضغط من قبل المتعاقد بما يفيد الموافقة (مرتين مثلا)، وذلك للتأكد من رغبته في التعاقد(٣). يضاف إلى ذلك أن إيجاب العميل لا يكتمل إلا بعد أن يقوم بالتوقيع الإلكتروني على العقد، الأمر الذي يتيح أمامه الفرصة للعدول عن العقد على الرغم من قيامه بالضغط على الأيقونة.

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 186; **Laura Darden, Charles Thorpe;** Op, Cit, p. 8.

(٢) **بشار طلال أحمد مومني**، المرجع السابق، ص٦٦.

(3) **Nicole Atwill**; Op, Cit, p. 8.

(ثانيًا) النطاق المكاني للإيجاب في العقود المصرفية على شبكة الإنترنت:

١٨١- نظرا لعالمية شبكة الإنترنت والتي تعد البيئة التي تعمل فيها البنوك الإلكترونية وتؤدى خدماتها فأن الإيجاب الذي يتم عبر هذه الشبكة بخصوص أحد العقود المصرفية من المفترض فيه ألا يكون مقيدًا بحدود جغرافية معينة.

لكن قد يجد البنك بعض العقبات في ممارسة نشاطه تجاه أفراد يقيمون في دولة معينة، كما لو كانت القوانين الرقابية داخل هذه الدولة تمنع ممارسة البنك لنشاطه داخل إقليمها، أو تمنعه من تقديم أنواع معينة من الخدمات المصرفية لاعتبارات معينة تقدرها، ففى مثل هذه الحالات يلجأ البنك إلى الحد من دولية نشاطه، من خلال قصر توجيه عروض خدماته على مناطق معينة[1].

لكن لاعتبارات الأمان بالنسبة للبنك الإلكتروني (خاصة المتعلقة بتنفيذ العقد والمنازعات التي يمكن أن تنشأ عنه) فإنه قد يلجأ إلى تحديد النطاق المكاني للإيجاب.

وقد ظهر تطبيق ذلك من قبل بعض البنوك الإلكترونية العاملة عبر شبكة الإنترنت في بريطانيا حيث تضمن كل العقود المصرفية المعروضة على موقع البنك على الشبكة بند يفيد بأن هذه القبول لهذه العقود لا يكون إلا من سكان المملكة المتحدة فقط.

(Applications only accepted from mainland residents of the

---

(١) د. أسامة أبو الحسن، مرجع سابق، ص ٧٦؛ د. فايز عبد الله الكندرى، مرجع سابق، ص ٦٠٥.

United Kingdom)[1].

ومن ثم يثور التساؤل حول الأثر القانوني لهذا التحديد المكاني للإيجاب في العقود المصرفية على شبكة الإنترنت؟

١٨٢- والأثر القانوني لهذا التحديد المكاني للإيجاب في العقود المصرفية على شبكة الإنترنت يتمثل في أنه إذا صدر الإيجاب من شخص يقع موطنه داخل النطاق المكاني المحدد لعرض البنك أعتبر إيجابا صحيحا يكفى صدور قبول من البنك لانعقاد العقد بموجبه. أما إذا صدر الإيجاب خارج النطاق المكاني المحدد لعرض البنك فلن ينعقد العقد. بل يجب أن يكون موطن الموجب داخل النطاق المكاني المحدد لعرض البنك. وكذلك الحال إذا كان هناك نطاق مكاني للتسليم في عرض البنك، فإن العقد ينعقد بقبول الإيجاب ويلتزم البنك الإلكتروني في هذه الحالة بتقديمها في النطاق المكاني المحدد للتسليم[٢].

- ونتفق مع جانب من الفقه[٣] على أنه على الرغم من أن إضافة مثل هذا الشرط للإيجاب من شأنه أن يضيق من نطاق عمل البنك الإلكتروني من الناحية الاقتصادية إلا أنه يحقق لها نوعا من الأمان من الناحية القانونية إذ لن يلتزم البنك بعقود في نطاق جغرافي وقانوني لن يسيطر عليه وخاصة أنه قد توجد بعض القوانين التي تتضمن حالات يحظر فيها التعامل أو قيودا أخرى وفقا لتصورها بشأن حماية المستهلك، لذلك قد تكون من مصلحة البنك الإلكتروني أن

(1) **FlexAccount Terms and Condition,** available at: http://www.nationwide.co.uk/ internetbanking/help/help_FlexAccount_Terms_and_Conditions.htm

(٢) د. **فريد عبد المعز فرج**، مرجع سابق، ص ٥٣٢.

(٣) د. **أسامة أبو الحسن**، مرجع سابق، ص٧٧.

يحدد نطاقا معينا للإيجاب.

المطلب الثالث

القبول في العقود المصرفية على شبكة الإنترنت

١٨٣- يعرف القبول وفقا للقواعد العامة بأنه الإجابة بالموافقة التامة على عرض الموجب، والذى بإضافته إلى الإيجاب يتكون العقد(١).

والأصل أن الموجه إليه الإيجاب له حرية القبول أو الرفض، لكن إذا قـرر القبول فإنه يجب توافر شروط معينة في هذا القبول حتى يعتد به، وينتج أثره في انعقاد العقد وهى:-

١- **مطابقة القبول للإيجاب في كافة عناصره:** حيث يجب أن يصدر القبول موافقا للإيجاب في كل عناصره، بحيث لا يتحقق القبول ومن ثم لا ينعقد العقد إذا اختلف القبول مع مضمون الإيجاب. ومن هنا لن يتحقق القبول إذا علق على شرط لم يتضمنه الإيجاب، ويعتبر بمثابة إيجاب جديد.

٢- **عدم سقوط الإيجاب وقت اكتمال الوجود القانوني للقبول:** بالإضافة إلى موافقة القبول للإيجاب، يجب تلاقى القبول بإيجاب قائم. والإيجاب القائم هو

---

(١) د. فتحى عبد الرحيم عبد الله، العناصر المكونة للعقد كمصدر للالتزام، مجموعة البحوث القانونية والاقتصادية – كلية الحقوق – جامعة المنصورة، مجموعة البحوث القانونية والاقتصادية – كلية الحقوق – جامعة المنصورة، العدد(٧)،١٩٧٨، ص ١٠٥

الذي لم يتحقق بشأنه حالة من حالات السقوط[١]. ومن ثم يمكن القول بأن القبول الذي يصدر بعد سقوط الإيجاب يعد إيجابا جديدا، يحتاج إلى قبول لانعقاد العقد[٢].

والقبول في العقود المصرفية على شبكة الإنترنت لا يخرج عن هذا المضمون، سوى في أنه يتم عن بعد عبر وسائط إلكترونية (شبكة الإنترنت)، لذلك فهو يخضع لذات الشروط التي تنظم القبول التقليدي[٣]، خاصة ما تعلق منها بمطابقة القبول للإيجاب في كل جوانبه[٤].

وهذا ما نظمته التشريعات الدولية والعربية من إمكانية التعبير عن الإيجاب والقبول عبر شبكة الإنترنت على نحو يرتب لهما ذات الأثر القانوني في حالة التعبير عنهما في الوسط المادي.

فقد نص قانون الأمم المتحدة النموذجي بشأن التجارة الإلكترونية "UNICTRAL"[٥] في المادة ١/١١ على أنه "في سياق تكوين العقود، وما لم

---

(١) ويسقط الإيجاب في حالات معينة هي: (أ) أن يعدل الموجب عن إيجابه (ب) إذا انقضى الأجل الذي حدده الموجب للإبقاء على إيجابه دون صدور قبول (٣) أن يرفض الإيجاب ممن وجه إليه. **د. فتحي عبد الرحيم عبد الله**، الوجيز في النظرية العامة للالتزامات، المرجع السابق ص ٧٥.

(٢) **د. أحمد شوقي عبد الرحمن**، مرجع سابق، ص٤٢.

(٣) **د. خالد ممدوح إبراهيم**، إبرام العقد الالكتروني،المرجع السابق، ص٢٦٧.

(٤) وفى هذا الصدد فقد نص العقد النموذجي الفرنسي للتجارة الإلكترونية في بنده السابع تحت عنوان "قبول العرض" أن موافقة المشترى يجب أن تتضمن تحديدا لبعض العناصر وهى الشيء أو الخدمة المتعاقد عليها والثمن، وطريقة الوفاء، وطريقة التسليم، وطريقة الصيانة بعد البيع. انظر في ذلك **د. فريد عبد المعز فرج**، مرجع سابق، ص٥٣٦.

(٥) **قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية**، ١٦ ديسمبر ١٩٩٦،

يتفق الطرفان على غير ذلك، يجوز استخدام رسائل البيانات للتعبير عن الإيجاب والقبول. وعند استخدام رسالة بيانات في تكوين العقد، لا يفقد ذلك العقد صحته أو قابليته للتنفيذ لمجرد استخدام رسالة بيانات لذلك الغرض".

أما القانون التونسي رقم ٨٣ لسنة ٢٠٠٠ بشأن المبادلات والتجارة الإلكترونية تنص المادة الأولى منه على أنه "يجرى على العقود الإلكترونية نظام العقود الكتابية من حيث التعبير عن الإرادة ومفعولها القانوني، وصحتها، وقابليتها للتنفيذ فيما لا يتعارض وأحكام هذا القانون"(١).

ولما كانت العقود المصرفية على شبكة الإنترنت لا تعدو أن تكون عقودًا إلكترونية من حيث الأصل فإنه سيسرى عليها الأحكام الخاصة بالقبول الإلكتروني بصورة عامة.

١٨٤- واستكمالا لما سبق أن ذكرناه بخصوص أن المتعاقد مع البنك هو الموجب في العقد المصرفي، فأن البنك في العقد المصرفي على شبكة الإنترنت يكون هو القابل. بعبارة أخرى لن يكتمل البنيان القانوني للعقد المصرفي على

منشورات الأمم المتحدة (A.99 v.4).

Available at: http://w.unCitral.org

(١) **وقد كان هذا هو موقف القانون الإماراتي رقم ٢ لسنة ٢٠٠٢ بشأن المعاملات والتجارة الإلكترونية** حيث نصت المادة الثالثة عشرة منه على انه لأغراض التعاقد يجوز التعبير عن الإيجاب والقبول جزئيا أو كليا بواسطة المراسلات الإلكترونية "و **في القانون البحريني الصادر في ١٤ سبتمبر ٢٠٠٢ بشأن التجارة الإلكترونية على انه** " في سياق إبرام العقود يجوز التعبير كليا أو جزئيا عن الإيجاب والقبول وكافة الأمور المتعلقة بإبرام العقد والعمل بموجبه، بما في ذلك أي تعديل أو عدول أو إبطال للإيجاب أو القبول عن طريق السجلات الإلكترونية ما لم يتفق الطرفان على غير ذلك".

شبكة الإنترنت بمجرد قيام المتعاقد بالضغط على أيقونة الموافقة والتوقيع الإلكتروني على العقد، بل يحتاج الأمر إلى موافقة البنك على هذا التعاقد، وذلك بعد أن يطمئن على توافر كافة المقومات محل الاعتبار بالنسبة له كشخصية العميل.

وغالبا ما يقوم البنك بالرد على هذا الإيجاب الموجه من قبل المتعاقد عن طريق إرسال رسالة إلكترونية (E-mail) يحدد فيها موقفه سواء بالقبول أم الرفض[١].

- حق عميل البنك الإلكتروني في إنهاء العقد المصرفي:

١٨٥- بعد أن يكتمل البناء القانوني للعقد المصرفي بتلاقي إيجاب وقبول أطرافه، فإن تساؤلا يطفو على سطح البحث يتعلق بمدى حق العميل في إنهاء هذا العقد.

والقول إجابة على التساؤل هو أن المشرع المصري سكت عن تنظيم حق العميل في إنهاء العقد المصرفي عبر شبكة الإنترنت بعد إبرامه.

أما على صعيد النظم القانونية الأخرى، فقد تصدى البرلمان الأوربي[٢]

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p.186.

(2) **Directives EC** 2000, (Distance Marketing of Consumer Financial Services), Official Journal of the European Communities, art.6 (1); SI 2004/2095. Available at: http://www.finance.gov.ie/ documents/publications/legi/si853.pdf

- ويلاحظ أن القانون الفرنسي الخاص بحماية المستهلك قد أورد نصا يعالج فيه حق المشتري في الانسحاب من عقد بيع السلع عبر شبكة الانترنت، وقد أعطى فيه للمشتري مهلة للانسحاب من العقد تقدر بسبعة أيام كاملة تبدأ من تاريخ استلامه

للإجابة عن هذا التساؤل، حيث ذهب إلى إعطاء المستهلك للخدمات المالية الحق في انهاء العقد (Right of Withdrawal) بعد إبرامه، ودون أن يفرض عليه جزاءات من قبل مقدم الخدمة المالية، ودون أن يكون العميل ملزمًا بتقديم أي أسباب قانونية لهذا الانهاء.

ولم يطلق هذا التوجيه الأمر على عنانه، بل قيد حق العميل في ذلك بقيدين[1]:

الأول: أن يعلن العميل عن رغبته في الانسحاب خلال ١٤ يوم من تاريخ إتمام التعاقد، وذلك من خلال إرسال إخطار إلى البنك يعرب من خلاله عن نيته في إلغاء العقد والانسحاب منه.

الثاني: ألا يكون أداء الأطراف قد اكتمل، بمعنى ألا يكون كل من طرفي العقد قد نفذ التزاماته تجاه الآخر.

وبناءً عليه، فإن العميل الذي أبرم مع البنك الإلكتروني أحد العقود المصرفية، يستطيع أن ينهى هذا العقد، مادام أنه عبر عن رغبته في ذلك خلال ١٤ يوما تالية لتاريخ إبرام العقد، ومادام لم ينتهي كل من البنك الإلكتروني والعميل من أداء ما عليه من التزامات بموجب العقد الذي يربط بينهما.

وفى حالة إنهاء العميل وفقا القيود سالفة الذكر، فإن المتعاقدين يعودان

للسلعة، وذلك دون أن يكون ملزما بتقديم أية أسباب لهذا الانسحاب.

Nicole Atwill; Op, Cit, p. 8.

(١) وقد راعت هذه التوجيهات عند إعطاء العميل هذا الحق، طبيعة سوق المال والخدمات المرتبطة به والتي تشهد تقلبات سريعة، تكون خارج السيطرة من عليها أو التحكم فيها، لذلك أعطى للمستهلك الحق في الانسحاب من التعاقد بينه وبين الجهة المزودة للخدمة متى أنه راعى القيود السالفة الذكر. انظر:

Apostolos Ath. Gkoutzinis, Op, Cit, p. 190.

الحالة التي كانا عليها قبل التعاقد، بمعنى أن يلتزم البنك الإلكتروني أن يرد للعميل كافة المبالغ التي يكون قد حصل عليها منه، أو ممن ينوب عنه وفقا لما هو محدد في العقد، متى كان ذلك ممكنا، على أن يتم ذلك خلال مدة لا تجاوز ٣٠ يومًا من تاريخ وصول الإخطار من العميل للبنك(١).

ويبدو لنا أن المدة التي منحها التوجيه الأوربي للعميل حتى يعلن عن رغبته في إنهاء العقد مدة كبيرة نسبيا، لا تحرص على تحقيق استقرار في التعاملات. وإن كان مما يخفف من غلواء هذه المدة ربطها بألا يكون العقد قد استكملت فيه أداء الأطراف.

والسؤال: هل يستطيع البنك الإلكتروني أن يستفيد من هذا النص ويقوم بإنهاء العقد المصرفي بعد انعقاده بذات القيود التي قررها التوجيه السابق.

١٨٦- الواضح من صياغة التوجيه أنها جاءت لتخاطب العميل أو المستهلك (Consumer)، كشكل من أشكال حماية هذا الطرف الضعيف في العلاقة التعاقدية، الأمر الذي لا يمكن معه القول باستفادة البنك الإلكتروني من هذا النص وإعطائه الحق في إنهاء العقد المصرفي بعد إبرامه، ويبرر ذلك أن الحاجة لإعطاء البنك مثل هذه المكنة لا تبدو ملحة. فطبيعة العقد تسمح له ألا يقبل التعاقد إلا بعد أن يستوثق جيدا من شخصية المتعاقد معه، ومن ضماناته المالية التي تؤهله للحصول على أحد الخدمات التي يقدمها، ومن ثم تبدو حاجة البنك لمثل هذا الحق ضعيفة.

يضاف إلى ذلك أيضا أن البنك غالبا ما ينص في العقود التي تحكم علاقته

---

(1) **Ibid.**

بعملائه على حالات يستطيع من خلالها أن ينهى علاقته بالعميل بعد انعقاد العقد المصرفي، على النحو الذي يمكن البنك من استخدام هذه الحالات في الوقت الذي يختل فيه ائتمان العميل بأي شكل مما قد تظهر معه حاجة البنك إلى إنهاء علاقته بهذا العميل(١).

---

(١) **انظر المادة الثامنة من شروط إصدار بطاقة ماستر كارد البنك التجاري الدولي CIB والتي تنص على أن** "تعتبر البطاقة ملكا للبنك، ويتعين على حامل البطاقة أن يردها بمجرد طلبها ويجوز لحامل البطاقة في أي وقت أن ينهى الاتفاق بينه وبين البنك بناء على طلب كتابي منه بإلغاء البطاقة ويتعين عليه إعادة البطاقة، ويجوز للبنك إلغاء البطاقة أو سحبها في أي وقت بدون إشعار مسبق كما يجوز رفض إعادة إصدارها أو تجديدها دون إبداء الأسباب وذلك كله دون الإخلال بحق البنك بالخصم من حساب العميل بالمديونيات الناشئة عن استخدام البطاقة وحتى تاريخ إعادتها للبنك أو الإخطار الكتابى".

HSBC, Internet banking terms and conditions,Processing your instructions, Op. Cit.

(We may suspend any service provided to you under the internet Banking Service without notice where we consider it necessary or advisable to do so…).

الفصل الثاني

تطبيقات للعمليات المصرفية على شبكة الإنترنت

١٨٧- عمليات البنوك بصورة عامة لا تقع تحت حصر، فهي متعددة ومتنوعة بل هي في تزايد مستمر بفعل العرف المصرفي من ناحية، وبفعل تطور أساليب ممارسة العمليات المصرفية من ناحية أخرى. والعمليات المصرفية المقدمة من قبل البنك العامل عبر شبكة الإنترنت لا تخرج عن هذا المعنى. فهذه البنوك ليست بنوكا متخصصة في تقديم أنواع معينة من العمليات المصرفية، بل هي بنوك تقدم كافة أشكال العمليات المصرفية، ولكن من خلال شبكة الإنترنت. بمعنى آخر أن البنوك الإلكترونية العاملة عبر شبكة الإنترنت تقدم كافة العمليات المصرفية التقليدية (من إيداع وسحب وتحويل إلخ) بالإضافة لبعض العمليات المبتكرة بفعل استخدام الإنترنت في تقديم هذه العمليات. لكن لا مجال هنا لعرض كل هذه العمليات هنا، وهذا يعود إلى أن القواعد القانونية الحاكمة لهذه العمليات لا تختلف كثيرا عن الأحكام الخاصة بالعمليات التقليدية.

ومن خلال هذا الفصل نحاول تسليط الضوء على نماذج لبعض العمليات المصرفية المبتكرة، أو التي كان لتقديمها عبر شبكة الإنترنت إضافة جديدة في أسلوب تقديم العمليات المصرفية، على أن نحيل بشأن العمليات التقليدية للمراجع العامة في عمليات البنوك مع التحفظ بشأن قواعد إبرامها (الإيجاب والقبول)، حيث يسرى عليها ما سبق ذكره في المبحث السابق مراعاة لطبيعة الوسيلة المستخدمة في الإبرام في هذه العقود.

وعلى ما تقدم، نعرض من خلال هذا الفصل لأهم التطبيقات لهذه العمليات على النحو التالي: إصدار النقود الإلكترونية (مبحث أول)، التحويل المصرفي الإلكتروني (مبحث ثان)، على أن يسبق ذلك عرض سريع لعقد يبرم بين البنك الإلكتروني والعميل خارج نطاق التعاقدات المصرفية ولكنه لازم للحصول على هذه العمليات، يسمح بمقتضاه البنك الإلكتروني للعميل بالدخول إلى موقعه وطلب الخدمات المصرفية الإلكترونية المختلفة وهو عقد تقديم خدمة الإنترنت، كل ذلك على النحو التالي.

١٨٨- عقد خدمة الدخول لموقع البنك عبر شبكة الإنترنت:

يعد عقد الدخول للموقع الإلكتروني للبنك على شبكة الإنترنت The Internet Service Agreement أول علاقة قانونية تجمع بين البنك والعميل، يمنح الأول بموجبه الثاني حق الدخول على موقعه الإلكتروني تمهيدا لحصوله على الخدمات المصرفية التي يقدمها من خلال هذا الموقع فهو بمثابة تصريح دخول يكون للعميل بموجبه صفة شرعية في ولوج موقع البنك، واستعراض خدماته والتعاقد على هذه الخدمات مع البنك، وذلك من خلال قيام البنك بتزويد العميل برقم تعريف PIN(١)، وكلمة دخول Password، خاصين به، للدخول إلى موقع البنك، وأيضا تزويد هذا العميل بكافة التعليمات والإرشادات الخاصة بالتعامل مع هذا الموقع وكيفية الاستفادة من الخدمات المصرفية التي يقدمها(٢).

---

(١) وهو عبارة عن سلسة من الأرقام تستخدم لتمييز المستخدم. انظر:
Internet Banking; Op. Cit, p. 79.

(2) **First Utahbank,** Internet access agreement, p 1 Available at: http://www. Firstutahbank.com/internet_access.html

١٨٩- ويكتسب عقد الدخول بهذا المعنى أهمية خاصة بالنسبة للبنك الإلكتروني، تتجلى في قدرة الأخير على إلزام العميل بالأسس العامة التي تحكم العلاقة بينهما، سواء فيما يتعلق بأسلوب تعامل العميل مع الموقع الإلكتروني للبنك، وما يفرض عليه من التزامات أمنية (مثل الالتزام بسرية البيانات، الالتزام بعدم الاعتداء على عناصر الملكية الفكرية الموجودة على موقع البنك(١)) في هذا الخصوص(٢)، أم بحصوله على الخدمات المصرفية التي يقدمها، وما يفرض على العميل من قواعد عامة تتعلق بالتعاقد المصرفي على خدمات البنك(٣).

وعلى الرغم من أن خدمة الدخول تعد خدمة غير مصرفية، إلا أنها أساس لجميع الخدمات المصرفية الإلكترونية التي يقدمها البنك الإلكتروني لعميله، حيث تبقى هذه الخدمة جنبا إلى جنب بالنسبة لكل خدمة مصرفية الكترونية، حيث يفترض قبل حصول العميل على أي خدمة مصرفية أنه تعاقد مع البنك على خدمة الدخول. وعقد الدخول بهذا المعنى يعد علاقة مستقلة بين البنك والعميل، يتضمن حقوق والتزامات أطرافه بخصوص تنظيم عملية الدخول والتعامل مع

Bank of internet USA, Website agreement, available at: http://www. bankofinternet.com/website-usage-legal-policy.aspx

(١) وقد تعرض أحد عقود الدخول الخاصة بأحد البنوك العاملة على شبكة الانترنت لتوضيح المقصود بعناصر الملكية الفكرية للبنك، بأنها عبارة عن كافة البيانات والمواد الموجودة على موقع البنك والتي يعتمد عليها في التعامل مع البنك عبر شبكة الانترنت، مثل العلامة التجارية للبنك، والعنوان الإلكتروني الخاص به، حيث يحظر على العميل محاولة نسخ هذه العناصر أو تحريفها بأي شكل.

Jyske bank, JBPB, Net Bank, user agreement, (EN)-2007, available at: http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf

(2) **Alain Hiltgen. Thorsten kramp. Thomas**; Op, Cit, p. 27.

(3) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 37.

موقع البنك الإلكتروني، وإجراءات الأمان التي يجب على العميل الالتــزام بهــا أثناء التعامل مع موقع البنك الإلكتروني، والإجراءات المتبعة في حالة حــدوث خلل أو عطل في عمل الموقع، وتنظيم المسؤولية في حالة حدوث استعمال غير مشروع من الغير(١).

وعلى الرغم من الأهمية التي يشغلها عقد الدخول بالمعنى السابق في علاقة البنك بعميله، إلا أن النظام القانوني المصري يخلو من نصوص تنظم هذا العقد، الأمر الذي تداركته النظم القانونية الأخرى، مراعية الطبيعة الخاصــة لخدمــة الدخول من كونها خدمة غير مصرفية تتسم بالطــابع الفنــي، وكونهــا خدمــة ضرورية لتقديم الخدمات المصرفية على شبكة الإنترنت. فقد ذهب مكتب الرقابة على النقد الأمريكي (OCC) إلى أن البنك الإلكتروني يستطيع تقــديم خــدمات إلكترونية غير مصرفية للعملاء طالما أنها مفيــدة ولازمــة لتقــديم الخــدمات المصرفية الإلكترونية(٢).

١٩٠- ويتمتع عقد الدخول في علاقة البنك وعميله بخصوصية معينة تتمثل في أمرين:

---

(1) **E-Banking,** Federal financial institutions examination council; Op. Cit, p. 5; **Apostolos Ath. Gkoutzinis**; Op, Cit, p36

(2) (The **OCC** has long held that national banks have an incidental authority to provide electronic products or services that can be used for both banking and non- banking functions as part of a package of banking related products or services where the full function products or services are not an excessive amount of the total package);

OCC Interpretive Letter No 742(August 19, 1996), Internet access service; **Internet Banking** Op, Cit, p. 1.

١) أن هذا العقد يعد بمثابة الشريعة العامة التي تحكم علاقة البنك بعميله، ومن ثم فإن أي بند أو شرط يرد في أي عقد مصرفي (بخصوص خدمة مصرفية يحصل عليها العميل) يخالف أي بند أو شرط ورد في عقد الدخول فإن العبرة تكون لما جاء في عقد الدخول ويلغى كل ما يخالفه.

٢) أن البنك يملك في أي وقت تعديل أي نص في هذا العقد، أو استبداله بآخر دون الرجوع إلى العميل، بل أن اعتراض العميل على هذا التعديل أو الاستبدال من شأنه أن ينهي علاقته بالبنك نهائيا(١).

ويبدو لنا أن احتفاظ البنك بمثل هذه الخصوصيات يبرره أهمية وخطورة الاعتبارات الأمنية في نظام عمل البنك العامل عبر شبكة الإنترنت. فمباشرة العمل المصرفي في بيئة إلكترونية مفتوحة على العالم بأسره، يقتضي تمتع البنك في مواجهة عميله ببعض السلطات الاستثنائية التي تمكنه من تعديل شروط هذا

---

(1) (In the event of a conflict between these terms and conditions and the Bank's standard terms and conditions relating to any account, the standard terms and conditions shall prevail)

(The Bank reserves the right to amend, vary, supplement or replace these terms and conditions of the User Agreement)

(If the User Agreement is amended, the revised User Agreement will be sent to you. You must accept the revised agreement by signing and returning the revised User Agreement. If you do not accept the agreement, you will not be allowed to access JBPB Net-bank)

-**Jyske bank**, JBPB, Net Bank user agreement, (EN)-2007; Op. Cit.

-**Bank of Internet USA**, Website agreement, available at: http://www.bankofinternet.com/website-usage-legal-policy.aspx

العقد أو استبدالها على النحو الذي قد تفرضه الظروف الأمنية، وأن يجعل هـذا العقد يجب أي شرط أو بند يرد في أي عقد مصرفي يخالفه. لكن يجب دائما أن يرتبط السماح للبنك باستعمال هذه السلطات بما تقتضيه فقط الاعتبارات السابقة، بمعنى ألا يطلق العنان للبنك في استعمال هذه السلطات على نحو يتعارض ومبدأ سلطان الإرادة. فعلى الرغم من أن العميل عند موافقته على عقد الدخول يعلم بتمتع البنك بهذه السلطات في مواجهته، إلا أن إرادته تنصرف في الغالب إلى أن هذه السلطات استثنائية، ولا يقبل أن يتمتع البنك بها بصورة مطلقة، الأمر الذي يقتضى أن يتم التعامل مع هذه السلطات بمبدأ أن الضرورة تقدر بقدرها.

١٩١- ويأتي في مقدمة الالتزامات الواقعة على عاتق البنك بموجب هذا العقد تمكين العميل من الدخول إلى موقعه عبر شبكة الإنترنت، والحصول على كافة العمليات التي يقدمها، بما يقتضيه هذا من تزويد هـذا العميـل بكافـة الأدوات والبرامج التي تساعده على هذا، وتوفير كافة المعلومات التي تمكنه من التعامـل مع هذه الأجهزة والبرامج، وذلك طبقا لما هو متفق عليـه فـي العقـد المبـرم بينهما(١).

وهذا ما نظمه قانون الصفقات الموحد الأمريكي، حيث عالج أحكـام هـذا العقد في المادة ٦١١ من هذا القانون، حيث ذهب إلى التزام البنك بتمكين العميل من خدمة الدخول في الوقت وبالأسلوب المتفق عليه في العقد المبرم بينهما(٢).

---

(1) **Firest Utahbank,** Internet access agreement, p 1 Available at: http://www.firstutahbank.com/internet_access.html

(2) **Uniform computer information transaction ACT**,(on uniform state laws), annual conference,Colorado,July23-30,1999.p48. available at:

وهذا الالتزام يفرض على البنك التأكد دائما من سلامة الشبكة الخاصة به، والمتصلة بشبكة الإنترنت، واختبارها بشكل دوري، وذلك حتى يوفر دخولاً سهلاً وآمنًا ومستمرًا للعميل(١). وهذا يقتضي أن يستعين بأجهزة وبرامج جيدة، وأن يراعى تناسب الطاقة الاستيعابية لهذه الأجهزة مع عدد العملاء وحجم العمليات المصرفية التي يقدمها؛ وذلك حتى لا يحدث ضغط زائد وتكدس في الدخول على الموقع بما لا يتناسب مع قدراته(٢). والتزام البنك بتمكين العميل بالدخول إلى موقعه التزام ببذل عناية، يقاس بمعيار التوقع المعقول في ضوء التكنولوجيا المتاحة في نفس ظروف البنك وخبرته في التعامل الإلكتروني عبر شبكة الإنترنت(٣)، فيسأل فقط عما يقع تحت سيطرته من أجهزة وبرامج، ولا تمتد مسئوليته لما يخرج عن سيطرته(٤)، ومن ثم لا يسأل البنك عن سوء عمل جهاز الكمبيوتر الخاص بالعميل، أو سوء اتصاله بشبكة الإنترنت.

وهذا ما يجرى عليه العمل في المملكة المتحدة حيث تلتزم البنوك الإلكترونية بتوفير الكفاءة وسلامة الأداء وذلك في ضوء ما يدخل تحت سيطرتها من أجهزة وبرامج بحيث لا يسأل البنك الإلكتروني عن حالات الخلل أو العطل الذي يحدث في الشبكة العامة (شبكة الإنترنت) ما لم يثبت تقصيره(٥).

---

http://www.law.upenn.edu/bll/archives/ulc/uecicta/uetast84.htm

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 36.

(٢) انظر نموذج لعقد دخول على الانترنت متاح على الموقع الإلكتروني التالي:
http://arabic.procom.dz/abonnement.htm

(3) **OCC interpretive letter, No 742**, Op, Cit, p. 37.

(4) **Firest Utahbank**, Internet access agreement, p 5; Available at: http://www.firstutahbank.com/internet_access.html

(5) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 37.

ويفرض الإتحاد الفرنسي للبنوك في فرنسا على البنوك الإلكترونية في أدائها لخدمات الدخول للإنترنت اتباع أفضل المعايير المتعلقة بأداء مثل هذه الخدمات[1].

ويمكن أن يبرر طبيعة التزام البنك بكونه التزامًا ببذل عناية وليس بتحقيق نتيجة في هذا الخصوص، بالقول بأن تمكين العميل من الدخول لموقع البنك عبر شبكة الإنترنت تتحكم فيه عوامل أخرى غير كفاءة شبكة البنك وقدرة أجهزته على استقبال العميل، حيث يتأثر هذا أيضا بكفاءة جهاز الكمبيوتر الخاص بالعميل، وكفاءة المودم الذي يستعمله، أيضا طبيعة الخطوط المشترك فيها، وحجم الضغط الواقع عليها، لذا فإن التزام البنك في هذا الخصوص هو التزام ببذل عناية.

١٩٢- وبالمقابل لالتزامات البنك السابقة فإن عقد الدخول يفرض على العميل العديد من الالتزامات، من أهمها التعامل مع أدوات الدخول وموقع البنك الإلكتروني طبقا لمعايير الاستخدام السليم والحفاظ على رقم التعريف وكلمة الدخول الخاصين به حتى يتسنى له التعامل مع البنك الإلكتروني من خلالهما، والالتزام بالاستعمال الشخصي لهذه الأدوات، على أن تنعقد مسئوليته العقدية في حالة مخالفة هذه الالتزامات بموجب العقد المبرم بينه وبين البنك.

ويحتفظ البنك بحقه في منع دخول العميل على موقعه إذا ما أخل بالتزاماته تجاه البنك، مع التزام الأخير بإعلامه في هذه الحالة، مع ذكر الأسباب التي

---

(1) Ibid.

دفعته لذلك[1].

(١) انظر نموذج لعقد دخول على الانترنت متاح على الموقع الإلكتروني التالي:
http://arabic.procom.dz/abonnement.htm

المبحث الأول

إصدار النقود الإلكترونية

١٩٣- بادئ ذي بدء تجدر الإشارة إلى أن التطور السريع في وسائل الاتصال وما واكبه من تطور في المعاملات التجارية، أدى إلى تغيير النقود من كونها ورقية أو معدنية ذات مقياس موحد للقيم، إلى نقود الكترونية(١)، لا يمكن لمسها ولا ثقل ولا زنة لها ولا تحتاج إلى خزائن لحفظها، حيث يمكن عرضها على شاشات الحاسبات. وقد حظيت هذه النقود بقبول دولي على مستوى الأشخاص والمؤسسات المالية التي تتعامل بها(٢).

وتعد الولايات المتحدة الأمريكية من أوائل الدول التي عرفت النقود الإلكترونية، وذلك بعد سلسلة من التطورات التي شهدتها وسائل الدفع الإلكتروني، لتكون النقود الإلكترونية هي أحدث هذه الوسائل(٣).

---

(1) **Julien le Clainche**, l`adaptation des droits du paiement français et américain aux nouvelles technologies, p. 15, provident du site: www.droit-ntic.com

(٢) د. **علي أحمد مرسي عثمان**،مرجع سابق، ص٢٠٣؛

- **peter spencer**, Regulation of the payments market and the prospect for digital money, BIS papers, No. 7, p. 69.

- **Haibo Huang**; Op, Cit, p. 1;**Simon Newman and others**; Op. Cit, p. 238

(٣) وقد عرفت اليابان هذه النقود عام ١٩٩٥، وذلك بعد أن وافقت لجنة تابعة لوزارة المالية تضم بعض المؤسسات المالية وبعض شركات الاتصال على إصدار هذه النقود. كما عرفت فرنسا هذه النقود عام ٢٠٠٠. د. **محمد إبراهيم محمود الشافعي**، الآثار النقدية والاقتصادية والمالية للنقود الإلكترونية، مؤتمر الأعمال المصرفية

١٩٤- وعملية إصدار النقود الإلكترونية تعد وافدا جديدا على العمليات المصرفية للبنوك، حيث شهدت معظم تشريعات دول العالم (أن لم تكن جميعها) استقرارا فيما يتعلق بالجهة المخولة بإصدار النقود بصورة عامة في هذه الدول[1]، حيث جرى العمل على قصر هذا الأمر على جهة حكومية تتبع الدولة، تقوم بإصدار النقود وفق ضوابط معينة تراعى فيها العديد من الاعتبارات السياسية والاقتصادية والقانونية، الأمر الذي دعانا للتساؤل حول مدى اعتبار إصدار النقود الإلكترونية عملا من العمليات المصرفية التي يمكن للبنك الإلكتروني العامل عبر شبكة الإنترنت القيام بها. وعلى فرض أن هذا الإصدار كان من العمليات التي يمكن لهذه البنوك أن تقوم بها، فما هي الضوابط التي تحكم عمل البنك في ذلك؟ وما هي الالتزامات والمسؤوليات الواقعة على عاتق أطراف هذه العملية؟

كل هذه التساؤلات تقتضى منا التعرض لها، وذلك من خلال تعريف هذه النقود وإبراز أهم خصائصها، وذلك للتعرف على مدى اعتبارها من عمليات البنوك من عدمه (مطلب أول)، ثم بيان الالتزامات الواقعة على أطراف عملية إصدار هذه النقود، والمسؤوليات الواقعة عليهم في ضوء هذه الالتزامات (مطلب ثانى).

الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص ١٤٧؛ د. **على أحمد مرسى عثمان**، مرجع سابق، ص ٢٠٤.

(1) **G C Chalikias**; Op, Cit, p. 1.

المطلب الأول

مدى اعتبار إصدار النقود الإلكترونية عملا مصرفيا

١٩٥- تقتضى حداثة عملية إصدار النقود الإلكترونية من ناحية، وتطلع بعض المؤسسات المالية غير المصرفية إلى إصدارها من ناحية ثانية، وجود اختلاف فقهي[١] حول اعتبار إصدار هذه النقود عملا مصرفيا، يمكن للبنك القيام به أم لا.

وللوصول إلى هذه الغاية، فإن الأمر يحتاج منا إلى التعرف على ماهية هذه النقود؛ في ضوء تعريفها، وبيان أهم الخصائص التي تتمتع بها، للنظر في مدى اعتبارها عملا مصرفيا.

- تعريف النقود الإلكترونية:

١٩٦- يستخدم مصطلح النقود الإلكترونية للإشارة إلى النظم الإلكترونية المؤمنة لتبادل المعلومات والوحدات النقدية الإلكترونية بشكل رقمي. وقد استخدمت العديد من المصطلحات للإشارة إلى اصطلاح النقود الإلكترونية، مثل العملة الرقمية (Digital Currency)، أو النقدية الإلكترونية (E Cash)، أو نقود الإنترنت (Cyber Money)، أو نقود الشبكة (Net Money)[٢]، أو النقود الرقمية (Digital Cash)[٣].

---

(١) **د.أحمد السيد لبيب**، الدفع بالنقود الإلكترونية، رسالة دكتوراه - كلية الحقوق - جامعة المنصورة، ٢٠٠٧، ص١٥٧.

(٢) **محمد سعيد أحمد إسماعيل**، مرجع سابق، ص ٢٤٠.

(3) **Roger Gerleroy Miler – Gaylord A. Jentz**; Op, Cit, P. 406; **Simon Newman and Gavin Sutter**; Op. Cit, p. 238.

وقد عرف جانب من الفقه[١] النقود الإلكترونية بأنها " تلك الوحدات التي يتم تداولها عبر الوسائل الإلكترونية".

لكن يؤخذ على هذا التعريف أنه خلط بين وسائل الدفع الإلكترونية كلها (بطاقات الائتمان- الشيك الإلكتروني – النقود الإلكترونية) وإحدى صورها وهى النقود الإلكترونية، بمعنى آخر قد توسع في تعريف النقود الإلكترونية على نحو يجعلها تشمل كل وسائل الدفع الإلكترونية.

وقد عرفها التوجيه الأوربي (١٨ سبتمبر ٢٠٠٠) في المادة الثانية منه بأنها عبارة عن قيمة نقدية مخزنة الكترونيا على جهاز الكتروني وتصدر بقيمة نقدية لا تقل عن المقابل الذي دفع للحصول عليها، وتكون مقبولة كوسيلة للدفع من غير من أصدرها[٢]..

وقد تأثر جانب من الفقه[٣] باتجاه التوجيه السابق، حيث عرفها بأنها عبارة عن "سلسلة الأرقام الإلكترونية التي تعبر عن قيمة معينة تصدرها البنوك التقليدية أو الافتراضية لمودعيها ويحصل عليها هؤلاء في صورة نبضات bits كهرومغناطيسية على كارت ذكي أو على الحاسب الشخصي لتخزن على القرص الصلب (Hard drive) ويستخدمها هؤلاء على الحاسب لتسوية معاملاتهم التي

---

(١) د. **محمد سعدو الجرف**، أثر استخدام النقود على الطلب على السلع والخدمات، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص٢٠٠.

(2) **Directive EU, 2000/46/,** Article (1), Official Journal of the European Communities, 18 September 2000, p. 40.

(٣) د. **السيد أحمد عبد الخالق**، البنوك والتجارة الإلكترونية، مجلة البحوث القانونية والاقتصادية- كلية الحقوق – جامعة المنصورة، ص ٢٥.

تتم عن طريقه".

لكن هذا التعريف منتقد؛ وذلك على أساس تركيزه أكثر من اللازم على الجوانب الفنية للنقود الإلكترونية(1)، وذلك على حساب إهماله لباقي الجوانب الهامة في تعريف هذه النقود، كالجانب القانوني، والذي يعكس مصدر وطبيعة قوة الإبراء التي تتمتع بها هذه النقود في التعاملات.

١٩٧- التعريف الراجح:

قبل أن نضع تعريفا دقيقا لهذه النقود، نعرض لوصفها من أهم الجوانب التي تتجاذبها(٢):

فهي من الناحية الفنية، عبارة عن بيانات إلكترونية محفوظة على دعامة إلكترونية (القرص الصلب في جهاز الكمبيوتر"Hard disk" أو الكارت الذكي "smart card")، يتم تبادلها بين الأطراف المتعاملة، وذلك عن طريق تواصل الأجهزة الإلكترونية.

ومن الناحية القانونية، فهي عبارة عن وحدات إلكترونية ذات قيمة مالية (بحيث تمثل كل وحدة قيمة مالية معينة)، مقبولة كوسيلة دفع في المعاملات لما لها من قوة إبراء، مصدرها اتفاق الأطراف المتعاملة (وليس القانونَ كالنقود التقليدية).

وبناءً عليه، يمكن أن نعرف هذه النقود بأنها عبارة عن وحدات إلكترونية ذات قيمة مالية، مقبولة كوسيلة للدفع من غير مصدرها، تحفظ وتتداول بين

---

(1) **Simon Newman, Gavin Sutter**, Op. Cit, p. 311.

(٢) **د. شريف محمد غنام**، محفظة النقود الالكترونية، مرجع السابق، ص ٣٣.

المتعاملين بها إلكترونيا، وتتمتع بقوة إبراء نهائية[١] مصدرها اتفاق المتعاملين بها.

١٩٨- خصائص النقود الإلكترونية:

وتتمتع النقود الإلكترونية بالمعنى السابق بخصائص معينة على التفصيل التالي:

١)- ذات قيمة نقدية مخزنة إلكترونيا:

النقود الإلكترونية نقود ذات قيمة نقدية حقيقية[٢]، يقبلها الأفراد في التعامل مقابل التنازل عن سلعهم وخدماتهم، أو حتى مقابل تحويلاتهم المالية[٣]، وذلك دون حاجة للتأكد من وجود وكفاية حساباتهم المصرفية (على خلاف بطاقات الائتمان)، حيث إنها تتمتع بقوة إبراء في التعامل مثل النقود التقليدية (الورقية والمعدنية)، لكنها خلافا لهذه النقود، عبارة عن بيانات مشفرة يتم وضعها على وسائل إلكترونية في شكل بطاقات بلاستيكية أو على ذاكرة الكمبيوتر الشخصي[٤].

---

(١) وهى في هذا تتشابه مع النقود التقليدية، وتختلف مع الأوراق التجارية (كالشيك، والكمبيالة) والتي على الرغم من أنها تقوم بوظيفة النقود في الوفاء إلا أنها لا تتمتع بقوة إبراء نهائية (مطلقة)، ولكنها قوة إبراء نسبية، حيث لا تتحقق عملية الوفاء بالفعل إلا بحصول الحامل للورقة التجارية على قيمتها من المسحوب عليه.

(2) **Report on electronic money**, European central bank, august 1998, p 7; **Marie Wright**, Authenticating electronic cash transactions, Computer Fraud &security, 1997, p 10.

(٣) د. **السيد أحمد عبد الخالق**، مرجع سابق، ص٢٥.

Julien le Clainche; Op. Cit, p. 15.

(٤) د. **محمد إبراهيم محمود الشافعي**، مرجع سابق، ص١٥٢.

٢)- <u>النقود الإلكترونية ليست متجانسة:</u>

وهذه الخاصية يكتسبها النقد الإلكتروني نتيجة قابليته للتجزئة، وهي خاصية تميز النقود الإلكترونية عن العملة التقليدية (الورقية والمعدنية)، وهذه الخاصية تعنى إمكانية تحديد حجم وحدات السداد، وعدد وحدات النقد الإلكتروني وقيمتها بشكل مستقل(١). فمثلا المشاركون في صفقات نقد إلكتروني في مصر يمكنهم تقرير أن الوحدة الأصغر من النقد التي يرغبون في التعامل بها تكون (جنيه واحد) والوحدة التالية قد تكون ١,٥ جنيه، وهكذا، وهذا التحديد يكون وفقا لرغبات المشاركين في عملية الدفع، وليس مقصورا على التجزئة التقليدية لنظام النقد العادي(٢).

٣)- <u>مقبولة كوسيلة للدفع من غير البنك الذي أصدرها:</u>

تتميز النقود الإلكترونية بأنها مقبولة كوسيلة للدفع والوفاء في مواجهة أشخاص غير البنك الإلكتروني الذي أصدرها(٣)، فهي تختلف بذلك عن الكوبونات التي تصدرها بعض الجهات لتسهل على عملائها التعامل معها بموجب هذه الكوبونات. فحائز النقود الإلكترونية يستطيع استعمالها للحصول على متطلباته المختلفة لدى جهات غير البنك الذي أصدرها(٤)، هذا وإن كان

Report on electronic money; Op. Cit, p. 7.

(1) **Julien le Clainche**; Op. Cit, p. 15.

(٢) **د. طارق عبد العال حماد**، مرجع سابق، ص ١٠٨؛ وفى نفس المعنى د. **شريف محمد غنام**، المرجع السابق، ص٣٧.

(3)**Report on electronic money**; Op. Cit, p. 7

(4) **Gennady Medvinsky, B. Clifford Neuman**, Net Cash: A design for practical electronic currency on the internet, Information Sciences Institute, University of Southern California,1993, p. 1; **Re-**

مصدر قبولها في التعامل هو اتفاق الأطراف المتعاملة بها.

٤)- وجود النقود الإلكترونية واستخدامها كوسيلة وفاء يتطلب وجود ثلاثة أشخاص:

هؤلاء الأشخاص هم المصدر (البنك الإلكتروني)، والعميل The Payer، والتاجر المدفوع له The Payee[١]. ولا يتماثل دور البنك الإلكتروني المصدر لهذه النقود الإلكترونية مع دور البنك المركزي الذي يصدر النقود الورقية التي تتمتع بقوة الإبراء القانونية Legal Tender[٢].

والسؤال الذي يستوقفنا بعد التعرف على مفهوم النقود الإلكترونية وبيان أهم خصائصها هو مدى اعتبار إصدار هذه النقود عملا مصرفيا من أعمال البنوك الإلكترونية العاملة عبر شبكة الإنترنت؟

١٩٩- المعلوم في مصر وكافة دول العالم أن عملية إصدار النقود من الأمور التي يقتصر القيام بها على سلطة نقدية حكومية، وذلك وفقا لمعايير وضوابط معينة، تهدف إلى تنظيم هذه العملية على النحو الذي يجعلها تتلاءم مع طبيعة وحال الاقتصاد القومي، بحيث يمكن القول أن عملية إصدار النقود مسألة سيادية تنظمها الدولة بقرارات سياسية، ولم يحدث أن نظم القانون هذه العملية باعتبارها أحد الخدمات المصرفية التي تقدمها البنوك. وهذا ما يجرى عليه العمل في مصر، حيث نصت المادة السادسة من القانون رقم ٨٨ لسنة ٢٠٠٣ من قانون

---

port on electronic money; Op. Cit, p. 7.

(1) **James E Backhouse**; Op. Cit, p. 30.

(٢) **د. شريف محمد غنام**، المرجع السابق، ص٣٦.

البنك المركزي والجهاز المصرفي والنقد على أن "يتخذ البنك المركزي الوسائل التي تكفل تحقيق أهدافه والنهوض باختصاصه، وله على الأخص ما يأتي: (أ) إصدار أوراق النقد وتحديد فئاتها ومواصفتها...".ونصت أيضا المادة (١٠٧) من ذات القانون على أنه "مع عدم الإخلال بأحكام القانون رقم ٥٠ لسنة ١٩٤٠ بشأن إصدار العملة الورقية يكون للبنك المركزي دون غيره إصدار أوراق النقد، ويحدد مجلس إدارة البنك فئات ومواصفات أوراق النقد التي يجوز إصدارها، ويجب أن تحمل أوراق النقد توقيع محافظ البنك المركزي"[١]. وعلى صعيد التشريعات الأوربية، نصت المعاهدة التأسيسية للاتحاد الأوربي في المادة (١٠٦) فقرة أولى على منح البنك المركزي الأوربي احتكارًا (Monopoly) فيما يتعلق بإصدار العملات النقدية في الاتحاد[٢].

ووفقا لهذه النصوص يمكن القول بأن إصدار النقود لا يعد من العمليات المصرفية التي يمكن للبنوك العادية (التجارية والمتخصصة) القيام بها.

لكن هل تعد النقود الإلكترونية نقودا بمفهوم النصوص السابقة، الأمر الذي يقصر إصدارها على البنوك المركزية، ومن ثم لا تعد من قبيل العمليات المصرفية، أم لا تعد نقودا في مفهوم هذه النصوص ومن ثم يمكن للبنوك الإلكترونية أن تقوم بها باعتبارها من العمليات المصرفية؟

٢٠٠- في الواقع يخلو النظام القانوني المصري من تشريع ينظم إصدار وتداول النقود الإلكترونية حتى الآن، على الرغم مما لهذا الأمر من أهمية قصوى، الذي

---

(١) **الجريدة الرسمية المصرية**، العدد ٢٤ مكرر، ٢٤ يونيه ٢٠٠٣،

(2) **Monetary and financial code,** Article L141-5, available at: http://195.83.177.9/upl/pdf/code_25.pd

أفسح المجال أمام رجالات الفقه كي يدلو كل بدلوه فيما يتعلق بالتنظيم القانوني لهذه النقود، خاصة ما تعلق منها بالطبيعة القانونية لها.

وقد ذهب جانب من الفقه[1] إلى عدم اعتبار النقود الإلكترونية نقودا قانونية عادية بالمفهوم الذي جاءت به النصوص السابقة، وإنما هي مجرد وسيلة دفع إلكترونية. وقد أسس هذا الجانب من موقفه على اعتبارات معينة، أهمها أن النظام الذي يحكم عمل هذه النقود يتطلب موافقة العميل على الخصم من رصيد حسابه الجاري بالقيمة التي يتيحها له البنك، كما يعطى البنك الحق في الحصول على عمولة نظير تقديم الخدمة، يضاف إلى ذلك أن هذه النقود لا تكون لها قوة إبراء إلا بعد تسوية قيمة المدفوعات التي تمت لدى كل من بنك المشترى وبنك البائع.

وذهب جانب آخر من الفقه[2] إلى القول بأن النقود الإلكترونية نوع جديد من النقود، تتمتع ببعض أوجه الخصوصية تجاه النقود التقليدية. وقد أبرز هذا الجانب أوجه الخصوصية في أمرين:

الأول: أن التاجر يطلب من البنك المصدر- بعد تحصيل الوحدات الإلكترونية من المستهلك- أن يحولها إلى نقود عادية (ورقية أو مكتوبة). ومن ثم هي تختلف عن هذه النقود الأخيرة.

الثاني: أن التاجر، وهو يطلب من البنك القيام بهذا التحويل، لا يقوم بدور الدائن

---

(١) **د. عدنان إبراهيم سرحان**، الوفاء(الدفع) الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص٢٩١.

(٢) **د. شريف محمد غنام**، المرجع السابق، ص ٣٨؛ **د. محمد إبراهيم محمود الشافعي**، المرجع السابق، ص ١٤٢.

بالنظر إلى المعاملة التي تمت بينه وبين العميل، ولكنه يطالبه بالتحويل بموجب الاتفاق المبرم بينهما، والذي يلزم البنك بتحويل هذه الوحدات الإلكترونية إلى نقود عادية.

ويبدو لنا أن الاختلاف بين الاتجاهين السابقين هو مجرد اختلاف ظاهري في خصوص الإجابة على التساؤل الذي سبق أن أثرناه، لا يدفعنا لترجيح أي منهما، حيث إن كل الرأيين انتهى إلى إجابة واحدة عن هذا التساؤل، وهي أن النقود الإلكترونية لا تدخل في مفهوم النقود كما عبرت عنه النصوص التي حصرت إصدار النقود على البنك المركزي وحده. فسواء كانت النقود الإلكترونية مجرد وسيلة دفع إلكتروني، أم كانت نوعًا جديدًا من النقود يتمتع بخصوصية في مواجهة النقود التقليدية فالنتيجة واحدة من وجهة نظرنا، وهي عدم سريان الحظر السابق على إصدار النقود الإلكترونية.

أما من ناحية مدى اعتبار إصدار هذه النقود من العمليات المصرفية، فوفقا للنظام القانوني المصري ليس هناك ما يمنع من إمكانية قيام البنك الإلكتروني بذلك. فسياسة المشرع المصري بخصوص تنظيم العمليات المصرفية قامت على أساس عدم حصر هذه العمليات في إطار محدد. بل ترك المجال مفتوحا أمام البنوك كي تطور من أنشطتها، وتبتكر أشكالا جديدة من هذه الأنشطة بما يتناغم مع إيقاع التجارة وتطوراتها[1]، الأمر الذي لا يمنع من اعتبار إصدار النقود

---

(١) والدليل على ذلك أن المشرع المصري في قانون التجارة رقم ١٧ لسنة ١٩٩٩ عزف عن وضع معيار معين للعمليات المصرفية. بل قام بذكر أمثلة لأهم هذه العمليات في الباب الثالث منه في المواد من ٣٠٠ إلى ٣٧٧. وهي : وديعة النقود والصكوك، تأجير الخزائن الحديدية، النقل المصرفي، الاعتماد العادي والمستندي، خطابات الضمان، الحساب الجاري.

الإلكترونية من قبيل العمليات المصرفية التي يمكن للبنوك الإلكترونية العاملة عبر شبكة الإنترنت أن تقوم بها، بل يمكن القول إن وجود البنك الإلكتروني على شبكة الإنترنت يجعلها أحق من غيرها في تقديم مثل هذه الخدمات، وذلك بحسب ما تضطلع إليه من مزايا توفرها لها هذه الشبكة.

ويؤكد ذلك كله موقف البنك المركزي المصري عندما سمح لهذه البنوك بإصدار النقود الإلكترونية كأحد الأنشطة التي يمكن لها القيام بها وقد صاغ لذلك مجموعة من الضوابط التي يجب أن تلتزم بها هذه البنوك لإصدار هذه النقود، وهي(١):

أ) أن يكون البنك مستوفيا للضوابط الرقابية التي تتعلق بمدى التزامه بكل من معيار كفاية رأس المال وأسس تصنيف القروض وتكوين المخصصات والتوازن في مركز العملات وتركيز التوظيفات لدى المراسلين في الخارج والتركز الائتماني.

- بل ذهب جانب من الفقه إلى أبعد من ذلك، بالقول أنه إذا كان هناك معيار يجب أن يتبع لتحديد الأعمال المصرفية فهو كون هذا العمل قد صدر عن مصرف، وأن ذات العمل لو صدر منفردا عن أية مؤسسة أخرى غير المصرف فهو من قبيل عمليات الاستثمار. ولا يعد عملية مصرفية لعدم صدورها عن مصرف. ويدلل هذا الفقه على موقفه بالقول إن بعض العمليات لا تدخل بطبيعتها في النشاط المصرفي، ولكنها تكتسب هذا الوصف فقط لصدورها عن مصرف، وذلك مثل تأجير الخزائن الحديدية، ووديعة الأوراق المالية. د. **علي جمال الدين عوض**، **المرجع السابق**، ص ٨.

(١) **الضوابط الرقابية للعمليات المصرفية الإلكترونية وإصدار وسائل دفع للنقود الإلكترونية**، البنك المركزي المصري، الجلسة المنعقدة بتاريخ ٢٨ فبراير ٢٠٠٢، ص٢، انظر العنوان التالي:

http://www.cbe.org.eg/public/Regulations%20of%20The%20Electronic%20Banking%20Operations.doc

ب) أن يتبع البنك مبادئ حصيفة لإدارة مخاطر إصدار وسائل دفع إلكترونية وأن يحدد تفصيلا أنواع وسائل الدفع التي يرغب في إصدارها والشروط المتعلقة بها وكذا مسؤوليات الجهات ذات العلاقة بهذه النقود والتي تشمل على مسئوليات البنك والعميل.

ج) إفصاح البنك المرخص له بإصدار وسائل دفع لنقود إلكترونية على صفحة web الخاصة به بما يفيد حصوله على ترخيص بذلك، ورقم وتاريخ الحصول عليه، مع ربط هذا الموقع بصفحة البنك المركزي المصري المعلن فيها عن أسماء البنوك المرخص لها بذلك من خلال (Hypertext Links) حتى يتحقق العملاء من صحة الترخيص.

د) أن يتم الحصول على موافقة العميل على الخصم من حسابه الجاري بالقيمة التي يتيحها له البنك إلكترونيا والعمولة التي يتقاضاها البنك لقاء ذلك.

ه) أن يقتصر إصدار وسائل دفع لنقود إلكترونية على الجنيه المصري فقط لعملاء البنك خصما من حساباتهم الجارية الدائنة بالجنيه المصري مع عدم السماح بإجراء عمليات مبادلة currency swap بغرض إتاحة مثل هذا الاستخدام.

وبناءً عليه يجب أن يتقيد البنك الإلكتروني بهذه الضوابط عند قيامه بإصدار النقود الإلكترونية، كأحد أهم الخدمات التي يمكن أن يقدمها على شبكة الإنترنت.

والملاحظ على صعيد التشريعات الأوربية أنها تجاوزت حدود التساؤلات التي سبق أن طرحناها؛ فهى لم تقصر إصدار النقود الإلكترونية على البنوك المركزية فقط، بل لم تكتف باعتبار هذا الأمر من قبيل عمليات البنوك، ومن ثم

تختص بها البنوك كأحد الأنشطة التي تنفرد بتقديمها للعملاء، بل ذهبت لأبعد من هذا، حيث اعتبرت عملية إصدار النقود الإلكترونية عملية ذات طبيعة خاصة، يمكن لمؤسسات الائتمان- وعلى رأسها البنوك ـ القيام بها[١].

وقد وضعت هذه التوجيهات مجموعة من الضوابط، التي يجب على المؤسسة التي تصدر النقود الإلكترونية الالتزام بها[٢]:

أ) أن مؤسسة الإصدار ملتزمة دائما بتحويل الوحدات الإلكترونية إلى نقود عادية، ويجب أن يوضح عقد الإصدار شروط هذا التحويل.

ب) يجب ألا يقل رأس مال مؤسسة الإصدار عن مليون يورو. ولا تقل الأموال الخاصة بهذه المؤسسة عن هذه الكمية. وفي أي وقت المؤسسة يجب أن تحوز أموالا تعادل أو تزيد على ما أصدرته من نقود إلكترونية بنسبة ٢%، وذلك لمدة ستة أشهر قادمة.

ج) هذه المؤسسات يجب أن يكون لديها استثمارات لا تقل عن مسؤوليتها المالية

---

(1) (Credit institutions - by virtue of point 5 of Annex I to Directive 2000/12/EC - are already allowed to issue and administer means of payment including electronic money and to carry on such activities Community-wide subject to mutual recognition and to the comprehensive prudential supervisory system applying to them in accordance with the European banking Directives).
Directive 2000/46/EC , Official Journal of the European Communities, 18 September 2000, p. 39; **Report on electronic money**; Op. Cit, p. 10

(2) **Andres Guadamuz**, Electronic money: A viable payment system?, School of Law, University of Edinburgh, p 5. avaliable at: www.era.lib.ed.ac.uk/bitstream/1842/2255/1/ electronicmoney.pdf

بخصوص النقود الإلكترونية. ويجب أن تكون أنشطة هذه المؤسسات آمنة وسليمة.

د) يجب أن تلتزم مؤسسات الإصدار بالتشريعات الخاصة بغسيل الأموال.

وعلى الرغم من أن الفلسفة الخاصة التي تبنتها التوجيهات الأوربية في خصوص إصدار النقود الإلكترونية لا تتعارض مع إمكانية قيام البنوك الإلكترونية العاملة عبر شبكة الإنترنت من القيام بهذا الأمر، بل تكون هذه البنوك ذات أحقية عن غيرها من المؤسسات الائتمانية الأخرى في القيام بهذا الأمر، وذلك بالنظر لما تمتع به من ضمانات وما تخضع له من إجراءات رقابية تؤهلها لهذا الأمر. إلا أننا كنا نود لو أن هذه التوجيهات لم تتوسع في مفهوم جهة الإصدار لهذا الحد، وكانت قصرت هذا الأمر على البنوك فقط؛ وذلك بالنظر إلى طبيعة عملية الإصدار وما يرتبط بها من مخاطر تضرب وبقوة في عمق الاقتصاد الوطني، وذلك على النحو الذي يحتاج في المؤسسة القائمة على عملية الإصدار أن تستجمع ضمانات خاصة، وضوابط معينة لا تتوافر إلا في البنوك.

وتجدر الإشارة إلى أن قيام البنك العامل عبر شبكة الإنترنت بإصدار النقود الإلكترونية سوف يضفى وصف العمل المصرفي على هذا الإصدار؛ بما يحمله هذا الوصف من معانى وخصائص وأثار؛ بمعنى أن عقد الإصدار من قبل البنك لن ينظر إليه على أنه عقد ذو طبيعة خاصة تمشيا مع مفهوم التوجيهات الأوربية سالفة الذكر، بل سيعد في هذه الحالة عملا مصرفيا بالمفهوم الذي سبق أن أشرنا إليه، وبذات الخصائص الخاصة بالعقود المصرفية على شبكة الإنترنت[1].

---

(١) انظر سابقا، ص ٣٠٩.

وإصدار النقود الإلكترونية من قبل البنك الإلكتروني بهذا المعنى يمكن أن يظهر على أحد شكلين[١]: النقود الإلكترونية السائلة، والتي تدار بواسطة برنامج للحاسب الإلكتروني، والنقود الإلكترونية المدمجة ببطاقة لدائنيه، أو ما يسمى المحفظة الإلكترونية.

(أ) النقود الإلكترونية السائلة Electronic Cash:

٢٠١- وهى عبارة عن أنظمة دفع مختزنة القيمة أو سابقة الدفع تمكن من إجراء عمليات الوفاء من خلال استخدام الحاسب الآلي وشبكة الإنترنت[٢]. وتتميز هذه النقود بأنها لا تحتاج إلى أدوات أو وسائل مادية[٣]، فهي وحدات إلكترونية محفوظة على الكمبيوتر الخاص بالعميل (customers home computer)، أو على شبكة الإنترنت (Safe online repository)، حيث يستطيع العميل استخدامها في شراء ما يرغب فيه من السلع والخدمات عبر شبكة الإنترنت، على أن يتم خصم ثمن هذه السلع والخدمات في ذات الوقت من هذه القيمة النقدية الإلكترونية المخزنة. ويطلق على هذه النقود أحيانًا اسم النقود الشبكية (Net Money)[٤].

وحتى يتمكن عميل البنك الإلكتروني من الحصول على النقود الإلكترونية

(1)**Report on electronic money**; Op. Cit, p. 7.

(٢) يخزن على هذا البرنامج قطع العملة الرمزية أو مجموعة المعلومات التي تدل على قيمة معينة. انظر د. **عدنان إبراهيم سرحان**، المرجع السابق، ص ٢٨٤.

(3) **Simon Newman and others**; Op. Cit, p. 238.

(٤) د. **محمد إبراهيم محمود الشافعي**، مرجع سابق، ص١٥٠؛

Report on electronic money; Op. Cit, p. 7.

السائلة فأن هذا يحتاج منه اتباع الخطوات التالية(١):

(١) يقوم العميل (المشترى) بإبرام عقد مع البنك الإلكتروني، يتيح له هذا العقد الحصول على برنامج خاص بإدارة النقد الإلكتروني (Cyber wallet) ليتم تشغيله على الحاسب الخاص به، ويمكن هذا البرنامج العميل من الاتصال بالحاسب الخاص بالبنك الإلكتروني المصدر للنقود الإلكترونية السائلة والمودع لديه حساب العميل، كما يقوم هذا البرنامج أيضا بحماية وحدات النقد الإلكتروني من المحو والنسخ، كما يقوم بحساب الأرصدة في ضوء عمليات اقتناء النقد الإلكتروني أو صرفه في عمليات الشراء(٢).

(٢) يقوم العميل بالحصول على النقد الإلكتروني من البنك الإلكتروني بالكمية المناسبة لاحتياجاته، وعادة ما تكون في صورة وحدات نقد صغيرة للغاية تسمى *Tokens*(٣). ويتم ذلك من خلال قيام هذا العميل بملء طلب لفتح حساب النقد الإلكتروني المعد لذلك على موقع البنك الإلكتروني، أو يرسل

---

(١) **رأفت رضوان**، مرجع سابق، ص٦٧؛ وفى نفس المعنى **محمد سعيد أحمد إسماعيل**، مرجع سابق، ص ٢٤٤؛ **د.أحمد السيد لبيب**، مرجع سابق، ص ١٠٥.

(٢) ويمكن الحصول على هذا البرنامج من خلال إحدى الشركات المتخصصة في ذلك مثل شركة ***cyber cash***، ***Digicash***، ***KLELine***، ***Paycash*** انظر لمزيد من التفصيل، **د.أحمد السيد لبيب**، المرجع السابق، ص١٠٥؛

Jon M. peha, Ildar M. Khamitov, Pay Cash: a secure efficient internet payment system, electronic commerce research and applications, Science Direct, 2004, p 382; **James E Backhous**; Op. Cit, p. 30.

(٣) وهى عبارة عن وحدات إلكترونية ذات رقم مسلسلة، يستخدمها العملاء لإجراء عمليات الشراء على أن يقدم التجار هذه الوحدات إلى بنك العميل للمعالجة والدفع. ويعالج البنك كل وحدة كما لو كانت شيكات مادية وهو يمنع إعادة استخدام الوحدات بمقارنة الأرقام المسلسلة. د. **طارق عبد العال حماد**، المرجع السابق، ص١٤٩.

إلى البنك الإلكتروني رسالة إلكترونية عن طريق البريد الإلكتروني تتضمن طلبا للحصول على النقد الإلكتروني، ثم يقوم العميل بإيداع القيمة المالية النقدية (عملة ورقية، معدنية) المراد تحويلها إلى نقود إلكترونية عن طريق أحد أجهزة الصرف الآلي التابعة للبنك(١). وبمجرد موافقة البنك الإلكتروني على الطلب، يقوم بإرسال نموذج قبول بفتح حساب للعميل متضمنا رقم التعريف الخاص به "Account ID" وكلمة المرور "password".

(٣) والخطوة الثالثة خاصة بالتاجر (البائع) الذي سيتعامل معه عميل البنك الإلكتروني، حيث يلزم أن يكون مشتركا لدى أحد البنوك الإلكترونية، ويحصل هو الآخر على برنامج خاص بإدارة النقد الإلكتروني، حيث يعمل على إدارة العمليات الخاصة بتسجيل المتحصلات وإضافتها إلى رصيد البائع (على الحساب الخاص به)(٢).

(٤) وهذه الخطوة خاصة بالدفع(٣)، حيث يقوم المشترى باتخاذ قرار الدفع من خلال النقود الإلكترونية بالقيمة المطلوبة، فيقوم برنامج إدارة النقد الإلكتروني الخاص بالعميل بالآتي:

(أ) اختبار الرصيد وهل يسمح بالسداد أم لا.

(ب) إذا كان الرصيد يسمح بالسداد فيقوم البرنامج باختيار وحدات النقد

---

(1) **James E Backhouse**; Op. Cit, p. 30.

(2) **Simon Newman and others**; Op. Cit, p. 237.

(٣) وذلك بعد أن يكون المشترى قد قام بتصفح مقر البائع، وقام باختيار السلعة التي يرغب في شرائها والتعرف على أسعارها وتجميع هذه الأسعار من خلال برنامج البيع الخاص بالبائع.

التي سيقوم بالدفع بها، حيث يتم تحديد هذه الوحدات بالرقم الخاص بكل وحدة وقيمتها في كشف خاص لإرساله إلى البائع عن طريق البنك الإلكتروني المصدر للعملة.

ولتجنب الاستخدام المتعدد (Multiple use) لذات وحدات النقد الإلكتروني، فإن أي كمية نقدية تمنح رقمًا سريًا مشفرًا(Encoded serial number)، وعند عودة هذه الكمية إلى البنك، فأن هذا الرقم السري يتم فحصه، بحيث لا تقبل هذه الكمية النقدية من قبل البنك إلا في حالة عدم سبق استخدام هذا الرقم السري من قبل[1].

(٥) يقوم البنك الإلكتروني بتلقي كشفًا الدفع من العميل (المشترى) ويتأكد من صحة النقود الإلكترونية بطرق للتأكد مختلفة (صحة الأرقام الخاصة بوحدات النقد الإلكترونية، أو أي بصمات إلكترونية..إلخ)، وبمجرد التأكد من صحة هذه الأرقام، يقوم بإرسال وحدات النقد الإلكتروني إلى البائع.

(٦) وفيها يتلقى برنامج إدارة النقد الإلكتروني للبائع كشف بالعملات الإلكترونية الموقعة من البنك الإلكتروني، حيث يقوم بإضافة وحدات النقد الجديدة بأرقامها وعلامات التأمين الخاصة بها إلى خزينة البائع الرقمية[٢].

(٧) يقوم برنامج إدارة النقد الإلكتروني الخاص بالبائع بإخطار المشترى بتمام السداد فيقوم نظام النقد الإلكتروني للمشترى بمحو هذه الوحدات المخصصة بهذا الكشف من رصيد المشترى بصورة نهائية.

---

(١) د. **أحمد السيد لبيب**، مرجع سابق، ص ٢٢٢.

(2) **James E Backhouse**; Op. Cit, p. 30.

ويلاحظ على هذا النظام أن كل عملية دفع تقتضى توثيق البنك الإلكتروني لصلاحية حساب النقود الإلكترونية الخاصة بالعميل، كما أن ما يتم قبضه من النقود الإلكترونية في كل عمليات الدفع الإلكتروني يجب أن يعاد دائماً للبنك الإلكتروني، بمعنى أن كل النقود المتبادلة تتم بمعرفة البنك الإلكتروني الذي أصدرها، كما أن كل عمليات التحويل من حساب النقود الإلكترونية تكون مسجلة، بحيث يمكن عند الحاجة اقتفاء أثر كل عمليات التسوية النقدية(١).

(ب) محفظة النقود الإلكترونية(٢) Electronic Purse:

٢٠٢- تعد محفظة النقود الإلكترونية Electronic Purse شكلا آخر من أشكال النقود الإلكترونية تصلح للوفاء بالمبالغ قليلة القيمة، تتميز عن النقود الإلكترونية السائلة في إمكانية استخدامها وجها لوجه (peer to peer) في المعاملات الحاضرة (مثل النقود التقليدية)، بالإضافة لإمكانية استخدامها في المعاملات عن

---

(١) د. عدنان إبراهيم سرحان، مرجع سابق، ص٢٨٦.

(٢) وتسمى بالفرنسية (le porte-monnaie electronique)، وقد سميت بهذا الاسم لأنها: أولاً تخزن فيها وحدات ذات قيم مالية تصلح لسداد أثمان السلع والخدمات مثلها في ذلك مثل المحفظة العادية التي تحتوى على نقود حقيقية. ثانياً: أنها محفظة إلكترونية على أساس أنها لا تحوى نقودا بالمعنى التقليدي (ورقية أو معدنية)، وإنما تحوى وحدات أو نبضات إلكترونية يتم نقلها إلكترونيا وتمثل قيمة مالية محددة. د. شريف محمد غنام، محفظة النقود الالكترونية، المرجع السابق، ص١٠.

Julien le Clainche; Op. Cit, p. 9.

- ولقد أصبحت محفظة النقود الإلكترونية الأكثر شهرة في أوربا واليابان والولايات المتحدة وبشكل خاص لدى طلبة الجامعات والمدن الجامعية، حيث تستخدم هذه المحفظة في حرم الكلية أو الجامعة (وذلك للدفع الإلكتروني لدى آلات البيع والتصوير والحاسبات المحمولة وخدمات الطعام والرسوم ومحلات الكتب، وحتى لدى التجار المحليين والمستقلين الذين هم خارج الحرم الجامعي). محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية المرجع السابق، ص٢٤٦

بعد (عبر شبكة الإنترنت)[١]. وقد ظهرت هذه الوسيلة الجديدة كثمرة للتزاوج بين تكنولوجيا المعلومات والاتصالات وتكنولوجيا الكروت الذكية، الأمر الذي هيأ الفرصة أمام البنك الإلكتروني للاستفادة من هذا التقدم المذهل في كل النوعين من التكنولوجيا وتكريسه في خدمة عملائها[٢].

ومحفظة النقود الإلكترونية عبارة عن بطاقة بلاستيكية[٣] تحتوى على معالج صغير جدا (chip)[٤]، وتستخدم في تخزين النقود لتستخدم في عمليات الشراء والخدمات عبر الإنترنت (On Line)، أو في نقاط البيع التقليدية (Off Line)[٥] بشرط وجود قارئ

(1) **peter spencer**; Op, Cit, p. 72; **Electronic money**, Report of the working party on electronic money(Group of ten): Op. Cit, p. 2.

(٢) د. **شريف محمد غنام**، محفظة النقود الالكترونية، المرجع السابق، ص١٢.

(٣) وهى عبارة عن بطاقة إلكترونية رقيقة يتم تخزين جميع البيانات الخاصة بحاملها عليها مثل الاسم، العنوان، أسم البنك الإلكتروني المصدر لها، أسلوب الصرف، المبلغ المنصرف وتاريخه، تاريخ حياة العميل المصرفية. ويتم تصنيع هذه البطاقة من لدائن معالجة بكثافة من السيلكون المكثف ومن وحدات chips والشرائح فائقة القدرة التي يمكن من خلالها تسجيل جميع المعاملات الخاصة بالبطاقة. انظر رأفت رضوان، مرجع سابق، ص ٥٤ ولمزيد من التفصيل انظر د. **طارق عبد العال حماد**، مرجع سابق، ص١٢؛

Peter Spencer; Op, Cit, p72; **Report on electronic money**; Op. Cit, p. 7.

(٤) وهذا المعالج يحتوى أما على مجموعة وصلات يتم توصيلها بصورة مادية بالقارئ الإلكتروني، أو قد تحتوى على جهاز إرسال واستقبال حيث يعمل هذا الجهاز لاسلكيا أي بدون التوصيل المادي.

Simon Newman and others; Op. Cit, p. 238.

(5) **online** means: you need to interact with electronic bank to conduct a transaction with a third party. **Offline** means: you can conduct a transaction without having to directly involve to electronic bank. **Jim Miller**, E-money mini-FAQ, release 2000, p 2.

إلكتروني مناسب للبطاقة. والبطاقة تحتوى على مقدار محدد القيمة سلفا من النقد الرقمي يتناقص مع الاستخدام في عمليات الشراء المختلفة، وتحتوى هذه البطاقة أيضا على شريحة تتضمن سجلا كاملا عن عمليات استخدام صاحب البطاقة للنقود الإلكترونية، وفى حالة محاولة استخدام مزدوج للنقود فأن عملية تحويل النقود لن تتم[١].

ويمكن تعريف محفظة النقود الإلكترونية بأنها "وسيلة دفع افتراضية تستخدم في سداد المبالغ قليلة القيمة بشكل مباشر أو غير مباشر"[٢].

وهناك دورة تشغيلية لمحفظة النقود الإلكترونية تمر بها على النحو التالي[٣]:

١) يقوم البنك الإلكتروني بتزويد العميل بالبطاقة الذكية ووحدات النقد الإلكتروني وذلك من خلال مليء الطلب المعد لذلك على موقع البنك الإلكتروني، أو يرسل العميل إلى البنك الإلكتروني رسالة إلكترونية عن طريق البريد الإلكتروني تتضمن طلبا للحصول على البطاقة الذكية والنقد الإلكتروني. وبعد قبول البنك الإلكتروني لهذا الطلب يتم تحويل وحدات النقد الإلكتروني (وهذه الوحدات الإلكترونية تحمل رقما مسلسلا وتاريخ انتهاء

---

(١) د. محمد سعدو الجرف،مرجع سابق، ص٢٠٠.

(٢) د. شريف محمد غنام، المرجع السابق، ص ١٢؛

Roger Gerleroy Miler – Gaylord A. Jentz; Op. Cit, p. 413

(٣) محمد سعيد أحمد إسماعيل، مرجع سابق، ص٢٤٨ انظر أيضا في كيفية عمل محفظة النقود الإلكترونية العنوان التالي:

http://ar.marocinfocom.com/detail.php?id=838

الصلاحية وموثقة عبر المفتاح الخاص بالبنك الإلكتروني)[1] من البنك الإلكتروني إلى بطاقته الذكية (وتسمى هذه الخطوة عملية شحن البطاقة)[2]. ويتم هذا الأمر عن طريق قيام العميل بإدخال البطاقة في وسيلة الشحن التي تكون متصلة بحساب العملة الإلكترونية الخاص به لدى البنك الإلكتروني، ثم يكتب رقم التعريف الشخصي (PIN)؛ حيث يكون لكل مستهلك رقم تعريف خاص لضمان عدم استعمال الحساب إلا من قبل صاحبه، والذي لا يكون متطلبا لعملية الدفع. بعد ذلك يحدد عدد الوحدات من النقد المطلوب تحميلها على البطاقة. وبتأكيد صحة المبلغ المطلوب تنتهي عملية شحن البطاقة ومن ثم تكون جاهزة للاستعمال[3].

٢) وعندما يريد العميل استعمال محفظة النقود الإلكترونية لشراء إحدى السلع سواء على الخط online أو خارجه offline فأنه يقوم بتحويل القيمة المخزنة من بطاقته إلى بطاقة التاجر.

٣) يقوم التاجر بعد ذلك بإيداع هذه القيمة لدى البنك الإلكتروني الذي يتعامل معه، وعلى أساس الوحدات الإلكترونية التي تم استلامها، فأن بنك التاجر يقوم بتسجيل القيمة في الحساب الدائن للتاجر، كما يمكن للتاجر أن يحتفظ بهذه الوحدات على محفظته على أن يقوم باستعمالها في تسوية معاملات

---

(١) **د. عدنان إبراهيم سرحان**، مرجع سابق، ص٨٧.

(٢) وهذا التحويل يمكن أن يتم أيضا من محفظة إلكترونية أخرى، أو من خلال التليفونات الذكيةsmart-phone، تليفونات الدفع العامة public pay telephones (وهى نظام متبع في بلجيكا فقط) أو وحدات شحن خاصة عبر شبكة الانترنت. لمزيد من التفصيل انظر. **د.أحمد السيد لبيب**، مرجع سابق، ص١٢٩.

(٣) المرجع السابق، ص١٣٠

أخرى[1].

وبناءً عليه، يقوم البنك الإلكتروني العامل عبر شبكة الإنترنت بإصدار النقود الإلكترونية بصورتيها السابق ذكرهما[2] باعتبارها عملا من الأعمال المصرفية التي يمكن له تقديمها لعملائه عبر شبكة الإنترنت.

المطلب الثاني

التزامات أطراف التعامل بالنقود الإلكترونية

٢٠٣- التعامل بالنقود الإلكترونية يفرض وجود علاقات قانونية بين ثلاثة أطراف؛ البنك الإلكتروني والعميل من ناحية، والبنك الإلكتروني والتاجر الذي يقبل التعامل بالنقد الإلكتروني من ناحية ثانية، والعميل والتاجر من ناحية ثالثة.

وعلى الرغم من هذا التعدد في العلاقات إلا أن جميعها يدور في فلك عملية مصرفية واحدة وهي إصدار النقود الإلكترونية، الأمر الذي نفضل معه عدم

(١) انظر العنوان التالي:
http://www.paycashwallet.com/consumer/TermsAndConditions.html

(٢) وعلى الرغم من أن هاتين الصورتين للنقود الإلكترونية متشابهتان؛ من حيث إن كلا منهما تمثل قيمة مالية إلكترونية مخزنة تعادل قيمة نقدية معينة، وأن كلا منهما يظهر في صورة بيانات مشفرة سواء في مرحلة التخزين أو الاستخدام، إلا انه مع ذلك يوجد بعض أوجه الفرق بينهما تتمثل في الوسيلة الإلكترونية المستخدمة لتخزين وحدات النقد الإلكتروني عليها (جهاز الكمبيوتر، البطاقة البلاستيكية)، والإجراءات الأمنية المتبعة لحماية هذه الوسيلة وما عليها من وحدات، وأيضا نطاق استعمال كلا منهما؛ حيث إن النقود السائلة لا تستخدم إلا عبر شبكة الانترنت، أما محفظة النقود فيمكن أن تستخدم عبر شبكة الانترنت، وفى التعاملات المادية المباشرة (Face to face).

التعامل مع كل علاقة على حدة، بل نعرض لالتزامات كل طرف في مواجهة باقي الأطراف نظرا للارتباط الشديد بين التزامات هؤلاء الأطراف.

وكما سبق أن ذكرنا النظام القانوني المصري يخلو من تشريع ينظم إصدار وتداول النقود الإلكترونية كإحدى العمليات المصرفية التي يقدمها البنك العامل عبر شبكة الإنترنت حتى الآن، الأمر الذي يدفعنا إلى معالجة الالتزامات المختلفة لأطراف عملية الإصدار في ضوء القواعد العامة في النظام القانوني المصري، والتشريعات التي عالجت هذا الموضوع، وفي ضوء نماذج العقود التي تحكم تقديم هذه الخدمة من قبل البنوك العاملة عبر شبكة الإنترنت، وذلك على النحو التالي:

أولا- التزامات البنك الإلكتروني:

٢٠٤- يلتزم البنك الإلكتروني عند إصدار النقد الإلكتروني والتعامل فيه بمجموعة من الالتزامات في مواجهة العملاء سواء كانوا مستهلكين أم تجارًا على النحو التالي:

١- تمكين العميل من التعامل بالنقد الإلكتروني:

٢٠٥- يأتي في مقدمة التزامات البنك الإلكتروني في مواجهة عملائه عند إصدار النقود الإلكترونية تمكينهم من استخدام النقد الإلكتروني. ويقصد بهذا الالتزام تخليق وحدات النقد الإلكتروني، وتزويد العميل بكل ما يمكنه من التعامل بها على نحو آمن وفعال[1]. ويكتسب هذا الالتزام أهمية خاصة في نظام عمل

---

(1) Avaliable at:
www.rand.org/pubs/monograph_reports/MR1005/MR1005.ch4.pd

النقود الإلكترونية لا تعرفه النقود التقليدية؛ حيث ينتهي دور البنك المركزي عند حد إصدار النقود التقليدية ليتولى الأفراد بعد ذلك استعمالها، الأمر الذي لا يتوافر بخصوص النقود الإلكترونية، التي تحتاج إلى تدخل البنك لإصدار هـذه النقـود وتيسير استعمال العميل لها. ويعود ذلك إلى الطبيعة الفنية والتقنية المهيمنة على نظام عمل هذه النقود، بما يفرض على البنك الالتزام بتوفير كل ما يلزم لذلك من أجهزة وبرامج ومعلومات لازمة لتمكين العميل من التعامل بالنقد الإلكترونـي. وهذا ما أكده قانون البنوك الفيدرالي الأمريكي رقم 81, 101 (August 19 1996).(١)

وحتى يتم تمكين العميل من هذا فأن البنك الإلكتروني يلتزم بعدة أمور على النحو التالي:

أ) تخليق وحدات نقد إلكتروني قابلة للتداول، وذلك بتحويل الوحـدات النقديـة المادية إلى نقود إلكترونية مساوية لها في القيمة، وتحمل أرقاما مسلسلة، ثم القيام بشحن أداة الدفع بهذه الوحدات.

ب) أن يسلم العميل أداة الدفع، سواء تمثلت في برنامج دفع إلكترونـي (cyber wallet) أو بطاقة ذكية (Electronic Purse) وذلك حتى يـتمكن مـن

---

(1) **Fed. Banking L. Rep. (CCH) 81, 101 (August 19, 1996)** (where a national bank was providing a closed stored value system to an institutional customer, the bank could as part of that service also provide system participants with certain hardware and software to be used for the stored value functions ; the equipment was not viewed as a separate product or service), available at: www.occ.treas.gov/interp/dec99/ca339.pdf

إجراء مدفوعاته إلى التجار من خلال هذه الأداة. وإذا كان العميل ينوى استخدام البطاقة الذكية عبر شبكة الإنترنت، فيجب على البنك أن يسلمه القارئ الخاص بها(١)، ويجب أن تكون هذه الأداة وقت تسليمها للعميل في حالة جيدة، وأن يختبر العميل مستوى الأداء الخاص بها قبل أن يقر باستلامها من البنك. بل يجب على البنك أن يحرص على هذا الأمر بنفسه باعتبار أن مستوى أداء هذه الوسيلة يؤثر بشكل مباشر في سمعته(٢). وغالبا ما يطلب البنك من العميل الإقرار باستلام هذه الأداة بعد تأكده من سلامتها، وذلك بالنظر إلى التزامه (العميل) بردها وهي في حالة جيدة عند نهاية التعاقد. والتسليم هنا يمكن أن يتم عبر شبكة الإنترنت، وذلك من خلال قيام البنك بتمكين العميل من تحميل برنامج الدفع على جهاز الكمبيوتر الخاص به، كما يمكن أن يتم من خلال قيام البنك بإرسال البطاقة الذكية للعميل ليتسلمها بصورة مادية. وعلى البنك أن يتحقق ويتأكد من صفة من يتسلم أداة الدفع، بحيث لا يسلمها إلا للعميل نفسه أو ممثله القانوني.

ج) على البنك الإلكتروني أن يسلم العميل كافة الوسائل اللازمة لاستعمال أداة الدفع. ويرتبط هذا الالتزام بسابقه (الالتزام بتسليم أداة الدفع) ارتباطا لا يقبل التجزئة؛ حيث لا يتمكن العميل من استعمال أداة الدفع إلا إذا تم إحاطته علما بكافة الجوانب الفنية والأمنية والقانونية المتعلقة باستعمال هذه الأداة. ومن

---

(١) د. **أحمد السيد لبيب**،المرجع السابق، ص١٧٣؛ انظر أيضا نموذج يقرر التزام البنك الإلكتروني بتزويد العميل بالأدوات التي تمكنه من استعمال أداة الدفع.

NetBank, How NetBank help to protect you, Available at: http://www.netbank.com/about_security_how_protect.htm

(2) **Ir. A. A. P. Schudelaro,** Electronic payment, Computer law & security report, Vol.17. No. 2. 2001, p 106.

أهم هذه البيانات؛ اسم المستخدم والرقم السري الخاصين بالعميل، بالإضافة إلى شرح وافٍ لكافة الخطوات التي يجب يقوم بها لاستعمال هذه الأداة بشكل صحيح (بما في ذلك تكلفة شحن الأداة، والحدود القصوى للشحن، ومقدار العمولة المستحقة للبنك عن كل عملية دفع تتم)(١) وكذلك طبيعة المعاملات التي يمكن أن تستخدم فيها بما في ذلك أسماء وعناوين المتاجر التي تقبل التعامل بهذه النقود. وأيضا كافة الاحتياطات الأمنية اللازمة لاستعمال هذه الأداة، وإحاطة العميل علما بكافة التزاماته ومسؤوليته الناشئة عن اتفاقه مع البنك.

هذا ولا يوجد بالنظام القانوني المصري نص ينظم التزام البنك العامل عبر شبكة الإنترنت بتمكين عميله من التعامل بالنقد الإلكتروني بالمعنى السابق.

أما على صعيد التشريعات الأخرى، فقد نص التوجيه رقم (٤) الصادر عن البنك المركزي في مالطا بخصوص تنظيم إصدار البنوك للنقود الإلكترونية(٢)

(١) د. شريف محمد غنام، المرجع السابق، ص١٣٧؛ وانظر أيضًا:

Benjamin Geva, Recent international developments in the law of negotiable instruments and Payment and Settlement Systems, Texas international law journal, VOL. 42:685, 2007, p 716.

(2) (b) "a description of the holder's and issuer's respective obligations and liabilities; this is to include a description of the reasonable steps that the holder must take to keep safe the electronic payment instrument and the means(such as a personal identification number or other code) which enable it to be used"

Central bank of Malta, Electronic payment services, Central bank of Malta Act (Cap. 204), Directive No 4 January 2008, p 3. available at:

على هذا الالتزام. أيضا أكدت لجنة بازل للرقابة على عمليات البنوك هذا الالتزام من خلال المبادئ الاسترشادية للرقابة على عمليات البنك الإلكتروني في المبدأ رقم ١١[١]. وقد ما نظمه أيضا التوجيه الأوربي الصادر عام ١٩٩٧ والخاص بوسائل الدفع الإلكتروني[٢]، حيث ذهب هذا التوجيه إلى التزام البنك الإلكتروني بضرورة تزويد العميل بالبيانات الخاصة باستعمال أداة الدفع، وتطلب التوجيه أن يعلم العميل بها ضمن الشروط والبنود الخاصة بالعقد الذي ينظم علاقته بالعميل. وأن يحدد بدقة مدى مسئولية العميل عن فقد أداة الدفع، والتزامه بالإخبار في حالة الفقد أو التلف.

ويبدو لنا أن تطلب التوجيه صياغة هذه البيانات في صورة بنود داخل العقد الذي يجمع بين البنك وعميله، وعدم الاكتفاء بأن تظهر هذه البيانات في صورة تعليمات يوصى بها البنك عميله، هو الرغبة في إضفاء الطابع الملزم للعقد على هذه البيانات، ومن ثم ترتيب المسؤولية العقدية عند إخلال أحد الطرفين بها.

هذا وقد ترجمت بعض العقود هذا الالتزام بالفعل ضمن بنود العقد، وتطلبت أن يعلم البنك عميله بكافة البيانات الخاصة باستخدام أداة الدفع، بل ذهبت إلى حد ضرورة حصول البنك على موافقة العميل(Client approval of program

---

www.centralbankmalta.org/site/retail_payment_services.html - 17

(1) **Basel committee on banking supervision,** Management and supervision of cross-border electronic banking activities, July 2003, P 7. www.occ.treas.gov/ftp/release/ 2001-42a.pdf

(2) **Commission recommendation,**Transactions by electronic payment instruments and in particular the relationship between issuer and holder, of 30 July 1997; http://www.legaltext.ee/text/en/T70030.htm

changes) عند قيامه بتعديل أو تغيير في البيانات الخاصة باستخدام أداة الدفع[1].

ونرى ألا تترجم كلمة «Approval» الواردة في العقد بمعنى الموافقة، ونرى أن المقصود منها إعلام وإخطار العميل بالتغييرات التي تطرأ على استخدام أداة الدفع؛ حيث إن البنك بحكم سيطرته على أداء الخدمة المصرفية، عادة ما يحتفظ لنفسه ببعض السلطات في مواجهة العميل، لا يملك الأخير في مواجهتها الاعتراض، إذا ما أراد أن يستمر في الحصول على الخدمة.

لكن ماذا لو جاء العقد خلوا من مثل هذا الالتزام ؟

يلتزم البنك بهذا الالتزام حتى ولو لم يرد ذكره صراحة بالعقد، حيث يجد مصدره في هذه الحالة فيما تقضي به قواعد حسن النية في تنفيذ العقود، هذه القواعد التي تظهر أولى تطبيقاتها في تعاون البنك مع عميله من خلال إعلامه[2] بكافة الجوانب الخاصة باستخدام الأداة؛ بالنظر إلى الطبيعة الفنية لهذه الأداة، وبالنظر إلى أن البنك في مركز أقوى من عميله بما يملكه من معرفة.

ولعل حرص البنك على تسليم أداة الدفع وما يرتبط باستخدامها من بيانات للعميل شخصيا، هو الذي يفسر تحميله المسؤولية للعميل عن كافة المدفوعات التي

---

(1) (All changes to programs used to process CLIENT's data affecting input, output, control, audit, or accounting procedures of CLIENT shall be made only with the approval of CLIENT).Available at: http://www.techagreements.com/agreement-preview.aspx?num=516688&title=Americorp%20-%20Data%20Processing%20Agreement

(٢) د. سعيد سعد عبد السلام، المرجع السابق، ص١١٢.

تتم باستخدام أداة الدفع بعد ذلك(١).

أ- يلتزم البنك الإلكتروني بتزويد التاجر بالنهايات الطرفية المناسبة لإتمام عملية الدفع. هذه النهايات تكون مزودة بمحفظة إلكترونية تختلف عن المحفظة الخاصة بالعميل. ووجه الاختلاف يتمثل في أن هذه المحفظة تستقبل الوحدات الإلكترونية الواردة من العميل فقط ولا ترسل. وإذا كان الدفع يتم عبر شبكة الإنترنت من خلال صفحة الويب المتجر الافتراضي "virtual corporations"(٢) الخاص بالتاجر، فعلى البنك الإلكتروني أن يزود هذا التاجر ببرنامج تلقى المدفوعات، بحيث يقوم التاجر بتثبيته على الصفحة الخاصة به، ليتمكن من تلقى وحدات النقد الإلكتروني عبر شبكة الإنترنت(٣)، ويجب أن يزود البنك هذا التاجر بكافة البيانات اللازمة للتعامل بالنقد الإلكتروني مع

---

(1) (During the Wallet installation process you will create your personal Cyphermint Account and you may select a password for your Cyphermint Wallet. The password is essential in protecting your Cyphermint money. Cyphermint does not collect or maintain passwords. Cyphermint is not responsible for the safe keeping of your password or for any losses you may incur as a result of the misuse of your password).

PayCash Term s & Conditions, Right/Responsibilities of cyphermint users, Available at: http://www.paycashwallet.com/consumer/TermsAndConditions.html

(٢) وهى عبارة عن الشركات أو المتاجر التي ليس لها وجود مادى حيث تعمل وتؤدى خدماتها عبر شبكة الانترنت، ويتم التعامل معها من قبل مستهلكين يتواجدون في مناطق جغرافية مختلفة وذلك عن طريق الاتصال بالانترنت.

Internet banking, Comptroller handbook, Op. Cit, p. 89.

(٣) د. **أحمد السيد لبيب**، المرجع السابق، ص١٧١.

عملائه.

- يلتزم البنك الإلكتروني بتأمين استخدام أداة الدفع. ويتحقق ذلك من خلال تزويد هذه الأداة بنظم تشفير عالية الكفاءة، وذلك على النحو الذي يضمن عدم استخدامها إلا من قبل المرخص له، والذي يحمل مفتاح الشفرة التي تمكنه من ذلك[١]. كما يجب على البنك أيضا أن يفرض على التجار الذين يقبلون الدفع بهذه الأداة تبنى نظم تشفير قوية، وذلك من أجل ضمان تأمين استخدام أداة الدفع في مراحل استخدامها المختلفة[٢].

والسؤال الذي يطرح نفسه على بساط البحث هو مدى مسئولية البنك الإلكتروني عن الأخطاء الفنية Panes Techniques التي قد تحدث أثناء عمل أداة الدفع.

يرى جانب من الفقه[٣] ضرورة أن يتحمل البنك الإلكتروني المسؤولية عن جميع الأضرار الفنية الناتجة عن استعمال أداة الدفع، سواء كانت ترجع إلى سوء في العمل أو الوظيفة أو ترجع إلى أخطاء فنية. ويبرر هذا الاتجاه موقفه بأن ذلك من شأنه أن يبث الطمأنينة في نفوس العملاء، ومن ثم سوف يشجعهم على أن يقبلوا على استعمال هذه الوسائل المتقدمة في عملية الدفع، دون الخوف من

(1) **Jyske bank**, JBPB, Net Bank user agreement, (EN)-2007, Op. Cit.

(2) **Gennady Medvinsky, B.Clifford Neuman**; Op. Cit, p. 1; **Haibo Huang**; Op, Cit, p. 17; **James E Backhouse**; Op. Cit, p. 30; **Directive 2000/46/EC**, Official Journal of the European Communities, Article (7).

(٣) **د. شريف محمد غنام**، المرجع السابق، ص١٣٧؛ انظر في نفس المعنى:
Ir.A.A.P. Schudelaro; Op. Cit, p. 106.

ضياع حقوقهم بسبب صعوبة إثبات مسائل فنية تتشابه فيما بينها، وتقل خبرة العميل بخصوص إثباتها. ويضيف قائلاً أن إقامة المسؤولية على هذا النحو من شأنها أن تكون دافعا للبنك إلى تبنى تكنولوجيا آمنة تعمل بشكل جيد، وتتفادى الأعطال الفنية، وتتجنب سوء العمل أو الوظيفة.

ونحن من جانبنا لا نتفق مع هذا الاتجاه، ونرى أن قيام مسئولية البنك من عدمه تتوقف على ما إذا كان الضرر ناتجا عن سوء عمل أداة الدفع، أم ناتجا عن الأعطال الفنية لأداة الدفع. فالضرر في الحالة الأولى يتحمل البنك الإلكتروني المسؤولية عنه كاملة، حيث يلتزم البنك الإلكتروني بتسليم العميل أداة دفع تعمل بشكل جيد، ومن ثم تقوم مسئولية البنك في حالة إذا ما تعلق الأمر بسوء عمل أداة الدفع.

أما إذا تعلق الضرر بعطل فني (كتعرض أداة الدفع لمجال كهرومغناطيسي أدى إلى تعطلها، أو إصابة برنامج الدفع بفيروس)، فأننا نفرق بين ما إذا كان البنك الإلكتروني قد اتخذ كافة الإجراءات التي من شأنها تفادى حدوث مثل هذا العطل، بأن أخبر العميل بطريقة عمل أداة الدفع وكيفية استعمالها والمحافظة عليها، هنا لا تقوم مسئولية البنك الإلكتروني عن الأضرار التي تحدث بسبب هذا العطل الفني (بل يكون العميل هو المسئول عن سوء استعمال أداة الدفع).

أما إذا لم يقم البنك الإلكتروني باتخاذ الإجراءات التي من شأنها تفادى حدوث مثل هذا العطل، فإن مسئوليته تقوم في هذه الحالة مادام لم يتوافر الغش أو الإهمال الشديد في جانب العميل. ونبرر موقفنا هذا بأننا كما نحتاج إلى تشجيع العملاء على التعامل بالنقود الإلكترونية، نريد أيضا أن نشجع البنك الإلكتروني على تقديم مثل هذه الخدمات، وهذا لن يتأتى إلا في ظل توفير نوع

من التوازن في مسؤوليات الأطراف، بحيث لا نفتح باب مسئولية البنك الإلكتروني على مصراعيه، ولا نجحف بحقوق العميل في ذات الوقت.

أما فيما يتعلق بصعوبة الإثبات في هذا المجال، فليس من الصعب على العميل أن يثبت قيامه باتخاذ كافة الخطوات اللازمة لعمل أداة الدفع، ولكنها لم تحقق النتائج المرجوة بسبب سوء عملها، وخاصة أن أداة الدفع توجد بحيازته، وتعمل على تسجيل البيانات المدخلة والمخرجة منها.

يضاف إلى ذلك أن المحكمة التي تتولى الفصل في النزاع غالبا ما تحيل بخصوص هذه المسائل الفنية المعقدة لأهل الخبرة والمتخصصين في هذا المجال على نحو لا يجعل مسألة الإثبات صعبة.

ويؤكد موقفنا هذا ما جاء في المسؤوليات الاسترشادية الواقعة على عميل البنك الإلكتروني، والصادرة عن البنك المركزي المصري[١]؛ حيث جاء في البند الخامس منها: "يتحمل العميل مسئولية سوء استخدام الخدمة الناتج عن عدم الالتزام بإجراءات الحماية أو الشروط والأحكام الواردة في العقد الذي تم إبرامه مع البنك بشأن العمليات المصرفية الإلكترونية، أو الناتج عن قيامه بالكشف عن إجراءات الحماية أو مخالفتها لدى الاستخدام".

فهذا النص يفترض مسئولية البنك عن كافة الأضرار التي تلحق العميل من جراء استخدام أداة الدفع سواء كان مصدرها خطأ البنك أم مجرد نشاطه، على أن تتوقف هذه المسؤولية عندما يكون مصدر الضرر سوء استخدام العميل وعدم التزامه بإجراءات الحماية المقررة من قبل البنك في عقد الاستخدام.

---

(١) الضوابط الرقابية للعمليات المصرفية الإلكترونية وإصدار وسائل دفع للنقود الإلكترونية، مرجع سابق، ص١١.

أيضا تعرضت الفقرة الأولى من المادة الثامنة من التوصيات الأوربية الخاصة باستخدام النقود الإلكترونية لتنظيم هذا الأمر في العلاقة بين المصدر والحامل(١)، حيث لم تطلق العنان لانعقاد مسئولية البنك عن كل حالات توقف أداة الدفع عن العمل، بل حصرت هذه المسؤولية في حالات محددة وهي:

أ- حالة عدم التنفيذ أو التنفيذ المعيب للصفقة التي يقوم بها العميل بسبب سوء عمل أداة الدفع.

ب-حالة الصفقات التي تتم باستخدام أداة الدفع من قبل شخص غير مخول بذلك، بسبب خطأ في إجراءات التوثيق المرتبطة باستخدام أداة الدفع.

ج- أي خطأ أو مخالفة تحدث من البنك يترتب عليها الانتقاص من حساب العميل، دون أن يكون مرتبطا باستخدام أداة الدفع.

وبمفهوم المخالفة لا يكون البنك مسئولا خارج هذه الحالات، الأمر الذي لا يمكن معه إطلاق القول بمسئولية البنك عن كافة الأضرار الفنية الناتجة عن استعمال أداة الدفع.

لكن يستوقفنا تساؤل يتعلق بفقدان العميل لبعض الوحدات النقدية ليس بسبب سوء عمل أداة الدفع، ولكن بسبب وجود عطل في الأجهزة الخاصة بالبنك، كعطل فى وصلات الاتصال، أو انقطاع فى التيار الكهربائى.

درج العمل في البنوك الإلكترونية الهولندية على تضمين عقود الخدمات

(1) **Commission recommendation 97/489/EC,** concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, 30 July 1997, (Article 8/1).

المصرفية التي تقدمها عبر شبكة الإنترنت بنودًا تقرر إعفاء البنك من المسؤولية عن عدم تقديم الخدمة في حالات وجود عطل في وصلات الاتصال (Malfunctions in communications link)، أو انقطاع التيار الكهربائي (Electrical power supply)[1].

لكن هذا الموقف لم يرق للبرلمان الأوربي (EC) الذي بادر بإصدار توصية (الفقرة الرابعة من المادة الثامنة)[2] تعالج هذا الإفراط والمغالاة من قبل هذه البنوك في تخليها عن مسؤوليتها، حيث ذهب إلى التزام البنك برد كافة المبالغ التي فقدها العميل بسبب عدم إتاحة الخدمة (of services unavailability) من قبل البنك في هذه الحالة.

ويبدو لنا أن كل من الاتجاهين السابقين قد نظرا فى تقرير المسؤلية عن فقد وحدات النقد فى حالة حدوث أعطال فى اجهزة البنك من زاوية تهمه:

فالبنوك الهولندية ترى أن انقطاع التيار الكهربائي أو غيره من الظروف المماثلة غالبا ما تحدثٍ بصورة مفاجئة، قد يغلب معها القول بأن الأمر خارج سيطرة البنك، ومن ثم لا يسأل عن هذه الظروف.

أما البرلمان الأوربى فهو ينظر تعطل أجهزة البنك بسبب انقطاع التيار الكهربائي أو غيره من الظروف المماثلة هى من قبيل المخاطر التي يسأل عنها البنك بالنظر إلى طبيعة الخدمات التي يقدمها، والبيئة التي يعمل فيها.

والأمر على هذا النحو يدعونا إلى عدم الانتصار المطلق لأي من هذين

(1) **Ir.A.A.P.Schudelaro;** Op. Cit, p. 108.

(2) **Commission recommendation;** 97/489/EC, 8/4

الرأيين، ومحاولة التوفيق بينهما. حيث يمكن القول بمسئولية البنك عن المبالغ التي فقدها العميل بسبب الاعطال التى لحقت بأجهزته، حتى لو كان ذلك بسبب انقطاع التيار بصورة مفاجئة، بالنظر إلى أن هذا الفرض من الأمور المتوقعة التي يجب على البنك أن يستعد لمواجهتها، من خلال وجود أجهزة بديلة تعمل مباشرة بمجرد انقطاع التيار الكهربائي، حيث أن غفلة البنك عن الاستعانة بمثل هذه الاجهزة لمواجهة مثل هذه الظروف يعد تقصير وإهمال من جانبه، ومن ثم يسأل عنه. أيضا يسأل البنك عن المبالغ المفقودة حتى ولو لم يثبت تقصيره أو إهماله، بإعتباره مسئولا عن الأضرار التى تلحق العميل بسبب حصوله على الخدمات التى يقدمها، حتى ولولم يثبت الخطأ فى جانب البنك (نظرية تحمل التبعة).

لكن إذا ثبت أن البنك اتخذ كافة الإجراءات الاحتياطية لمواجهة مثل هذه الأمور، وأن ما حدث كان خارج سيطرته وتوقعه، وذلك على النحو الذي يظهر فيه هذا العطل على أنه سبب أجنبي يستحيل توقعه أو دفعه، فلا مسئولية على البنك في هذه الحالة.

٢- الالتزام بتمكين العميل من إيقاف عمل أداة الدفع والإبلاغ عن فقدها وإخطار التاجر بذلك:

٢٠٦- بالنظر إلى الطبيعة المنقولة لأداة الدفع الإلكتروني (سواء برنامج الدفع، محفظة النقود)، فإن احتمالية سرقتها أو ضياعها أمر وارد، بما قد يؤدى إلى استخدام هذه الأداة بصورة غير مشروعة، بما يلحق الضرر بالعميل صاحب هذه الأداة. الأمر الذي تبدو معه أهمية تمكين العميل من إيقاف عمل هذه الأداة في

مثل هذه الظروف(١)، وفي وقت مناسب. ويظهر التزام البنك بهذا الأمـــر فـــي اتجاهين(٢):

الأول: في مواجهة العميل، وذلك بأن يزوده بكافة الأجهزة والأدوات التي تمكنه من غلق أداة الدفع كلية، وإبلاغ البنك بصورة سريعة بهذا الغلق. ويجب أن يستفهم البنك من العميل عن أسباب غلق أداة الدفع، وذلك حتى يتعامل البنك مع كل حالة في ضوء أسبابها. فقد يكون سبب الغلق فقدان أداة الـــدفع، أو سرقتها أو كان الأمر مقصورا على سرقة رقم التعريـــف "Account ID" الخاص بالعميل فقط، أو "كلمة المرور "password"، أو حدث تهديـــد أو فشل كلى في استعمالها، أو استخدمها الغير بناء على غش أو تحايل، وذلك تفاديا لاستعمال أداة الدفع بطريقة غير مشروعة من قبل الغير.

الثاني: في مواجهة التاجر، وذلك بإخطار التاجر بأن أداة الدفع الخاصة بالعميل قد تم غلقها. وتبدو أهمية إخطار التاجر بذلك في امتناعه عن قبول استخدام أداة الدفع كوسيلة للوفاء في مواجهته. ويجب أن يتضمن هذا الإخطار على كافة البيانات المتعلقة بأداة الدفع المفقودة، مثل الرقم الخاص بهـــا، واســـم العميل صاحب هذه الأداة، وتاريخ الفقد، وأية بيانات أخرى تفيد في التعرف على هذه الأداة وصاحبها.

---

(1) (12): "you may close your Account at any time by clicking on the "Remove Funds" tab in your Wallet" **PayCash Terms & Conditions,** Right and Responsibilities of cyperment users, provision Available at : http://www.paycashwallet.com/consumer/ TermsAndConditions.html

(٢) د.**شريف محمد غنام**، محفظة النقود الالكترونية، المرجع السابق، ص ١٣٩.

ويلاحظ أن الإخطار بفقد أداة الدفع، سواء الموجه من العميل للبنك، أم الموجه من البنك للتاجر الأصل فيه أن يكون إخطارا كتابيا يتضمن البيانات الخاصة بأداة الدفع والعميل. لكن هذا لا يمنع من إحاطة المراد تبليغه علما بوسيلة أسرع (كالتليفون، الفاكس)، وذلك حتى يتخذ التدابير اللازمة لتجنب الاستخدام غير المشروع لهذه الأداة، إلى أن يصل إليه تبليغ كتابي بواقعة الفقد.

ويجب على البنك الإلكتروني أن ينص في العقد المبرم بينه وبين العميل على الطرق التي يمكن من خلالها للعميل الاتصال بالبنك بأسرع وسيلة ممكنة، كأن يضمن العقد أرقام التليفونات أو الفاكسات الخاصة بالبنك، وكذلك العنوان البريدي له، حتى يتسنى إبلاغ البنك بذلك[1]، وقد ذهب جانب من الفقه[2] وبحق إلى القول بأن الإخطار يكون قد تم من لحظة إبلاغ الموجه إليه به (بالتليفون، الفاكس)، وما الإخطار الكتابي إلا وسيلة لإثبات واقعة الإبلاغ، وليس وسيلة لوجود أو صحة هذا الإبلاغ.

وانطلاقا من أهمية التزام البنك بتمكين العميل من إيقاف أداة الدفع، وما يقابله من التزام العميل بإخطار البنك بهذا الإيقاف، يطفو على سطح البحث تساؤل يتعلق بتحديد الشخص المسئول عن الأضرار الناتجة عن الاستعمال غير المشروع لهذه الأداة في حالة فقدها.

لا يوجد في النظام القانوني المصري نص يجيب على هذا التساؤل.

ولقد أجابت بعض البنوك الإلكترونية في كل من هولندا والمملكة المتحدة

(1) **Jyske bank**, JBPB, Net Bank user agreement, (EN)-2007; Op.Cit.

(٢) د. **شريف محمد غنام**، محفظة النقود الالكترونية، المرجع السابق، ص ١٤٩.

عن هذا التساؤل وهي بصدد صياغة العقود الخاصة بإصدار النقود الإلكترونية، حيث ذهبت إلى تحميل العميل المسؤولية كاملة عن كافة الخسائر التي تحدث قبل إخطار البنك بفقد أداة الدفع، على أن يتحمل البنك المسؤولية بداية من وصول هذا الإخطار إليه[(١)].

لكن هذا الأمر لم يكن ليرق للبرلمان الأوربي الذي استشعر وجود نوع من الإجحاف بالعميل في مثل هذه الحالة، الأمر الذي دفعه إلى إصدار توصية حملت رقم (١٩٩٧/٤٨٩)[(٢)]، قرر بموجبها وضع حد أقصى لمسؤولية العميل عن الخسائر التي تتم قبل الإخطار، بألا تتجاوز ١٥٠ يورو، على أن يتحمل البنك ما زاد على ذلك. وقد ربط البرلمان الأوربي استفادة العميل من هذا الحكم بقيدين:

الأول: عدم صدور غش (Fraudulently) من قبل هذا العميل.

الثاني: أن يقوم العميل بإبلاغ البنك بإيقاف أداة الدفع خلال مدة ثلاثة أيام من تاريخ وصول كشف الحساب المصرفي له (حيث سيتضح له من خلال هذا

---

(1) **Ir.A.A.P.Schudelaro**; Op. Cit, p. 108.

(2) **Commission recommendation 97/489/EC**, Article 6/1

- وقد تبنت بعض الشركات المقدمة لخدمات الدفع بالنقود الإلكترونية (**paycash-moneo**) هذا الموقف، حيث وضعت حدا أقصى لمسئولية العميل عن المبالغ المفقودة في الفترة الواقعة ما بين فقد أداة الدفع وتمام عملية الإخطار، حيث قدرت شركة **Moneo** المبلغ بـ ٢٧٥ يورو، وقدرت شركة **paycash** المبلغ بـ ٥٠ يورو. راجع د. أحمد السيد لبيب. المرجع السابق، ص ١٨٧؛

:https://consumers.paycash.us/CAM/Resources/Paycash%20terms%20and%20Conditions.pdf

http://www.moneo.net/fileadmin/user_upload/PDF/Conditions-Utilisation-Moneo-Vert.pdf

الكشف وجود استعمال غير مشروع للحساب الخاص به)، هــذا بالإضــافة لتحمل البنك المسؤولية كاملة عن الخسائر التي تحدث بعد الإخطار.

وقد أضافت الفقرة الثالثة من ذات المادة حكما يقرر عدم مسئولية العميــل مطلقا في حالة ثبوت عدم مراعاة البنك لإجراءات التوثيــق الإلكترونــي قبــل استعمال أداة الدفع.

ويبدو لنا أن كلاً من البنوك الهولندية والبريطانية من ناحيــة، والبرلمــان الأوربي من ناحية آخري قد نظر في تقرير المسؤولية من زاوية خاصة تهم كل واحد منهما على حدة. فالبنوك أرادت أن تنفى كل مسئولية عــن عاتقهــا فــي المرحلة السابقة على الإخطار حتى ولو كان الاستعمال غير المشروع لأداة الدفع يعود إلى عدم إتباع البنك لإجراءات التوثيق.

والبرلمان الأوربي أراد حماية الطرف الضعيف فــي العلاقــة التعاقديــة (العميل)، وذلك من خلال وضع حد معين لمسؤوليته عن الخسائر حتى ولو كان فقدان أداة الدفع يعود إلى تقصير وإهمال من جانبه. ولكننا ننظر لهذا الأمر من زاوية مختلفة، حيث نرى التفرقة بين مرحلتين في هذا الخصوص، الأولى بعــد قيام العميل بإخطار البنك، حيث تنعقد مسئولية البنك كاملة عن الخسائر التي تتم في هذه المرحلة، حيث تنتقل التبعة على عاتقه بموجب هذا الإخطار، والثانية قبل الإخطار، حيث تقرر المسؤولية في هذه المرحلة في ضوء السبب الذي أدى إلى إيقاف أداة الدفع. فإذا كان الإيقاف يعود إلى تقصير البنك في اتبــاع إجــراءات التوثيق الخاصة بمستخدم أداة الدفع أو بسبب سوء عمل أداة الدفع، أو نقص في المعلومات التي زود البنك بها العميل لاستخدام أداة الدفع والمحافظة عليها، هنــا تنعقد مسئولية البنك كاملة عن هذا الإيقاف. أما إذا كان الــسبب وراء الإيقــاف

يعود إلى إهمال العميل في المحافظة على أداة الدفع وما يرتبط بهـا مـن اسـم المستخدم أو كلمة المرور، هنا تنعقد مسؤوليته كاملة عن الخسائر التي تحدث من جراء هذا، ولا يتحمل البنك من هذه المسؤولية شيئًا مادام لم يحدث من جانبـه تقصير.

والسؤال: ماذا لو تحايل العميل وتظاهر بفقد أداة الدفع رغبة في الاسـتيلاء على أموال البنك؟

لاشك أن هذا الفرض يثير المسؤولية الجنائية للعميل عن جريمة النـصب، وذلك لقيامه باستخدام وسائل احتيالية بغرض الاستيلاء على أموال البنك بغيـر وجه حق، مما يتحقق معه وفقا للقواعد العامة في قانون العقوبات جريمة النصب بركنيها المادي والمعنوي.

وفى واقع الأمر، لم يفرد المشرع المصري نصا خاصا باستعمال الوسـائل الإلكترونية في ارتكاب جريمة النصب. لكن من خلال النظر في نـص المـادة ٣٣٦ من قانون العقوبات المصري نلاحظ أنها تستوعب إمكانية وقوع جريمـة النصب بالوسائل الإلكترونية حيث جاء في عجز هذه المادة: "يعاقب بالحبس كل من توصل إلى الاستيلاء على نقود أو عـروض أو سـندات ديـن أو سـندات مخالصة أو أي متاع منقول، وكان ذلك بالاحتيال لسلب كـل ثـروة الغيـر أو بعضها باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كـاذب أو واقعة مزورة. ..."

فالمشرع استعمل عبارة "طرق احتيالية" بلفظ عام، يمكن أن يندرج تحتـه استعمال الوسائل الإلكترونية من الكمبيوتر وشبكة الإنترنت في ارتكاب جريمـة

النصب، مادام أن من شأن هذه الوسائل الاحتيالية خديعة البنك وإيهامه(١).

لكن ذهبت بعض التشريعات الأخرى إلى إفراد نص خاص ينظم وقوع جريمة النصب باستخدام الوسائل الإلكترونية. من ذلك قانون العقوبات الياباني، حيث نصت المادة (٢٤٦/٤) على أن يعاقب كل من استعان بمعلومات مبرمجة كاذبة أو أدخل هذا النوع من المعلومات في نظام كمبيوتر لشخص آخر للحصول لنفسه أو للغير على ربح غيز مشروع(٢).

وقد أقر القضاء الفرنسي أيضا إمكانية وقوع جريمة النصب باستعمال الوسائل الإلكترونية. فقد قضى بأن أي تلاعب في مستندات البنوك يشكل وسيلة احتيالية تقع بها جريمة النصب، سواء أكانت المستندات ورقية أم بيانات مسجلة في الكمبيوتر، لما لهذه المستندات من مصداقية يترتب عليها تسليم المال في تلك الجريمة(٣).

---

(١) د. **السيد عتيق**، جرائم الانترنت، دار النهضة العربية، ٢٠٠٢، ص٧٣.
- وقد نص المشرع في قانون العقوبات المصري على طرق ثلاثة يمكن أن تقع بهما **جريمة النصب**، بحيث إذا لم تتوافر طريقة من هذه الطرق، لا تقع جريمة النصب وهي : ١- استعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة أو إحداث الأمل بحدوث ربح وهمى أو تسديد المبلغ الذى أخذه بطريق الاحتيال، أو إيهامهم بوجود سند دين غير صحيح أو سند مخالصة مزور ٢- التصرف في مال ثابت أو منقول ليس ملكا للجانى ٣- اتخاذ اسم كاذب أو صفة غير صحيحة. انظر د. **هشام محمد فريد رستم**، مرجع سابق، ص٢٦٩.

(٢) د. **شيماء عبد الغنى محمد عطا الله**، مرجع سابق، ص٧٥.

(٣) كما ذهبت محكمة باريس الابتدائية بحكمها الصادر في ١٦ ديسمبر سنة ١٩٩٧ إلى أنه يعد من الوسائل الاحتيالية الإلكترونية استعمال كلمة المرور للدخول إلى برنامج يسمح بالحصول على أموال الغير.
Anne Lise **VILARRUBLA**, L escroquerie et le web, 16 oct.2002.
مشار إليه لدى د. **شيماء عبد الغنى محمد عطا الله**، المرجع السابق، ص٧٧؛ انظر

ولا يؤثر في المسؤولية الجنائية للعميل بالمعنى السابق ثبوت خطأ البنك في إجراءات التوثيق اللازمة، أو غيرها من صور الخطأ[1].

والسؤال: هل من المتصور وقوع جريمة النصب في مواجهة البنك العامل شبكة الإنترنت؟

إذا كان الثابت وفقا لما تقرره القواعد العامة في قانون العقوبات المصري أن قيام الشخص باستعمال وسائل احتيالية للحصول على أموال مملوكةٍ للغير تقع به جريمة النصب[2]، فإن هذا مقرر لحالة قيام شخص باستعمال هذه الوسائل في مواجهة شخص آخر (إنسان)، الأمر الذي لا يتحقق في حالة قيام المعتدى باستعمال الوسائل الاحتيالية في مواجهة البنك العامل عبر شبكة الإنترنت (والذي هو عبارة عن مجموعة من الأجهزة الإلكترونية التي تعمل عبر شبكة الإنترنت)، ومن ثم القواعد العامة في قانون العقوبات غير قادرة على أن تستوعب هذه الحالة، كما لا يمكن قياس الاحتيال على الجهاز بالاحتيال على الإنسان، وذلك لامتناع القياس في المجال العقابي.

وهذا ما دفع بالعديد من التشريعات العقابية إلى التدخل بنصوص خاصة

أيضا د. **السيد عتيق**، مرجع سابق، ص ٧٤.

(١) د. **غنام محمد غنام**، الوجيز في شرح قانون العقوبات، القسم الخاص، (بدون تاريخ نشر)، ص ٧٢٨.

(٢) تنص **المادة ٣٣٦** من قانون العقوبات المصري على أن "يعاقب بالحبس كل من توصل إلى الاستيلاء على نقود أو عروض أو سندات دين أو سندات مخالصة أو أي متاع منقول وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها إما باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة أو إحداث الأمل بحصول ربح وهمى أو تسديد المبلغ الذى أخذ بطريق الاحتيال أو إيهامهم بوجود سند دين غير صحيح أو سند مخالصة مزور..."

لمواجهة هذه الحالة(١)، والتسليم بوقوع جريمة النصب في حالة مباشرة الوسائل الاحتيالية في مواجهة الأجهزة. وقد صاحب موقف هذه التشريعات أحكام القضاء أيضا، والتي سلمت بإمكانية وقوع جريمة النصب في هذه الحالة(٢). ومن ثم فإننا نهيب بالمشرع المصري بضرورة التدخل بنص خاص ينظم فيه إمكانية وقوع جريمة النصب إذا كانت الوسائل الاحتيالية مستخدمة في مواجهة البنك العامل عبر شبكة الإنترنت.

٣- التزام البنك الإلكتروني بتحويل النقود الإلكترونية إلى نقود عادية:

٢٠٧- ويقصد بهذا الالتزام تعهد البنك الإلكتروني بالاستجابة لمطلب العميل بتحويل ما في حوزته من وحدات النقد الإلكتروني إلى نقود تقليدية (معدنية أو ورقية) مكافئة لها في القيمة، وهو ما يطلق عليه عملية الاسترداد (Redemption)(٣).

ولا يوجد بالنظام القانوني المصري نص ينظم التزام البنك بهذا الأمر،

---

(١) ففى كندا نظم قانون العقوبات في المادتين ٣٨٧، ٣٨٨ حالات الاحتيال عن طريق التلاعب في الأنظمة الإلكترونية لمعالجة المعلومات، وكذلك في الولايات المتحدة الأمريكية وفقا للقانون الفيدرالى للاحتيال السلكى، فإن من ينتحل هوية غيره لاستعمال نظام حاسب معين يعد مجرما يمكن معاقبته وفقا لهذا القانون. انظر د.هشام محمد فريد رستم،المرجع السابق، ص ٢٧٣ وما بعدها.

(٢) حيث قضت محكمة التمييز الكويتية بوقوع جريمة النصب في حالة قيام المتهمة بانتحال صفة غير صحيحة، وهى أنها صاحبة الحساب، ولها الحق في السحب من حسابى المجنى عليهما مما حمل كلا من البنكين على تسليمها المال عن طريق جهازه الآلى يكفى وحده في لتكوين ركن الاحتيال، بما يكفى لوقوع جريمة النصب تامة. انظر تمييز ١٩٩٠/٥/٢٨ طعن رقم ٨٩/٢٤٢. مشار إليه لدى د. شيماء عبد الغنى محمد عطا الله، المرجع السابق، ص٧٢

(3) **Andres Guadamuz**; Op, Cit, p. 2.

وذلك على عكس الحال في النظم القانونية الأخرى. فقد نظم هذا الالتزام التوجيه الأوربي الخاص بتنظيم النقود الإلكترونية الصادر سنة ٢٠٠٠ في المادة الثالثة[١]، حيث ذهب إلى أن حامل النقود الإلكترونية أن يطلب من مصدرها أن يحولها إلى نقود قانونية عند سعر التعادل أو أن يحولها إلى حسابه الخاص، وذلك دون تحمل مصاريف أو رسوم غير تلك التي تكون ضرورية لتنفيذ هذه العملية.

وهذا الالتزام من قبل البنك يبرز خصوصية النقود الإلكترونية في مواجهة النقود التقليدية. فالأخيرة لا يوجد التزام بتحويلها إلى أي شكل آخر مكافئ لها في القيمة، وذلك على عكس النقود الإلكترونية التي يلتزم فيها البنك بهذا الالتزام. ويقف وراء تبرير هذا الالتزام أسباب عدة، منها ما يتعلق بحماية الاقتصاد القومي[٢]، ومنها ما تقتضيه طبيعة النقود الإلكترونية. فقبول هذه النقود في التعامل مستمد من ضمان البنك لها، الأمر الذي يدفعه إلى تشجيع التجار على

---

(1) **Directive 2000/46/EC**, Official Journal of the European Communities, Art.(3)
(A bearer of electronic money may, during the period of validity, ask the issuer to redeem it at par value in coins and bank notes or by a transfer to an account free of charges other Than those strictly necessary to carry out that operation.)

(٢) حيث إنه في حالة عدم وجود علاقة بين النقود الإلكترونية والنقود التقليدية فإن من شان هذا أن يغرى المؤسسات الائتمانية على التمادي في إصدار النقود الإلكترونية بلا حدود مما يؤدى في النهاية إلى خلق ضغوط تضخمية على اقتصاد الدولة، علاوة على ذلك فإن تعهد المصدرين بتحويل النقود الإلكترونية إلى نقود تقليدية سوف يقلل من خطر فقدان النقود الإلكترونية لوظيفة النقود باعتبارها وحدة محاسبية في حالة ما إذا لم تقبل المؤسسات الائتمانية تغييرها عند سعر التعادل. انظر د. **محمد إبراهيم محمود الشافعي**، المرجع السابق، ص١٧٥

قبول الوفاء من خلالها (حيث على قدر التزام البنك الإلكتروني بهـذا الالتـزام سيكون قبولهم للتعامل مع النقد الإلكتروني) بما يدفع البنك إلى الالتزام بتحويلها إلى نقود عادية. علاوة على كل ذلك فإن عملية التحويل هذه ما هي إلا استرداد التاجر لأموال سبق أن دفعها العميل من قبل إلى البنك(١).

ويتم هذا الأمر من الناحية العملية بطريقتين(٢):

الأولى: عن طريق أجهزة الصرف الآلي (ATM) التابعة للبنـك الإلكترونـي، حيث تسمح هذه الأجهزة بإمكانية إجراء عمليات الإيداع والسحب عـن بعـد وبصورة إلكترونية، بما يتلاءم مع طبيعة عمل البنك الإلكتروني.

الثانية: من خلال التحويل الإلكتروني على حساب العميل لدى أي بنك تقليدى.

والجدير بالذكر أن التزام البنك بالاسترداد ليس مقصورا على العميل فقط، لكن في مواجهة أي حائز شرعي للنقود الإلكترونية أيا كانت صفته، أي سـواء

---

(١) وقد أخذ التوجيه الأوربي هذه الاعتبارات عندما نص على ضـرورة التـزام البنـك الإلكتروني بالاسترداد، وذلك تدعيما لثقة الحامل، وإعادة هذه الوحدات إلى عمـلات نقدية أو قيدها في حسابه.

- (It is necessary for electronic money to be redeemable to ensure bearer confidence. Redeemability does not imply, in itself, that the funds received in exchange for electronic Money shall be regarded as deposits or other repayable funds for the purpose of Directive 2000/ 12/EC.

- (The issuance of electronic money may affect the stability of the financial system and the smooth Operation of payments systems.)

Directive 2000/46/EC, Official Journal of the European Communities, 18 September 2000, p39

(2) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 30; **Is auditing guideline internet banking**; Op. Cit, p. 2.;**G C Chalikias**; Op, Cit, p. 40.

كان العميل أم كان التاجر الذي تسلمها في مقابل ما قدمه من سلع وخدمات. ويستوي في ذلك أن يكون الطلب بالتحويل في صورة عملات معدنية أو ورقية، أو في صورة قيد في الحساب المصرفي الخاص بالحائز. وهذا ما نص عليه التوجيه الأوربي (٢٠٠٠/٩/١٨) في المادة الثالثة منه(١).

وإذا كان التزام البنك بعملية الاسترداد أمرًا لا خلاف عليه، لكن هذا لا يمنع من إعطائه الحق في تنظيم هذه العملية في بنود العقد وفقا لما يتلاءم مع ظروف عمله؛ كأن يشترط أن يقدم طلب الاسترداد خلال مدة معينة، أو أن يتم بعملة معينة، أو يضع حدا أدنى لا يقبل الاسترداد بأقل منه(٢). لكن يجب أن يتقيد في كافة الأحوال بالضوابط الخاصة بحماية المستهلك، فلا ينظم عملية الاسترداد على نحو يفرغها من مضمونها، بما يشكل إجحافا بحقوق العميل(٣).

والأصل أن البنك الإلكتروني ملتزم بتحويل النقود الإلكترونية إلى ما يعادلها من النقود التقليدية، والاستثناء على ذلك هو الامتناع عن التحويل في حالة ضياع أو سرقة أداة الدفع، وبشرط أن يكون العميل قد أخطر البنك بواقعة الفقد، حيث إن أي تحويل يطلب منه بعد هذا الإخطار، هو من قبل الحامل غير

---

(1) **Directive 2000/46/EC** Official Journal of the European Communities, Article (3).

(٢) لكن التوجيه الأوربي سالف الذكر قد اشترط ألا يقل هذا الحد عن عشرة يورو.

- (The contract may stipulate a minimum threshold for redemption. The threshold may not exceed EUR 10). **Directive 2000/46/EC**, Official Journal of the European Communities, Article (3,3).

(٣) د. عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الانترنت، مرجع سابق، ص ٧٩.

الشرعي لأداة الدفع. ومن ثم يجب عليه الامتناع عن التحويل في هذه الحالة(١).

وتجدر الإشارة إلى أن النقود الإلكترونية لا تخضع للتقادم، ولا تحمل تاريخ انقضاءExpire date، فهي صالحة للاستخدام حتى يتم تحويلها إلى نقود تقليدية. وبناء عليه لا يوجد ميعاد محدد يلتزم فيه الحائز بطلب الاسترداد، بل يلتزم البنك الإلكتروني بالرد مادامت النقود الإلكترونية في حوزته(٢).

ويبدو لنا أن التزام البنك بتحويل النقود الإلكترونية إلى نقود عادية يتأثر وجودا وعدما بمصدر إلزامية هذه النقود في التعامل. فمادام مصدر هذه الإلزامية هو اتفاق الأطراف المتعاملة فسيبقى لهذا الالتزام أهميته. أما إذا استلهمت هذه النقود قوتها الإلزامية في التعامل من القانون، فإنه لن يكون هناك أهمية لالتزام البنك بتحويل النقود الإلكترونية إلى عادية.

وأخيرًا يثور تساؤل حول إذا ما أفلس البنك الإلكتروني ولم تتم عملية الاسترداد.

الأصل أن العميل يعتبر دائنا للبنك بالوحدات الإلكترونية التي في حوزته (بموجب العقد الذي يلزم البنك بتحويل الوحدات الإلكترونية إلى نقود تقليدية)، ومن ثم يشترك العميل مع جماعة الدائنين في التنفيذ على أموال البنك بما له من ديون.

لكن ذهب اتجاه إلى القول بأن البنك يجب عليه في خصوص النقود الإلكترونية أن يعين كفيلا خاصا (بنك آخر) يضمن القيام بعملية التحويل في

---

(١) د. شريف محمد غنام، المرجع السابق، ص١٤٢.
(٢) د. أحمد السيد لبيب،المرجع السابق، ص١٧٧.

حالة عجزه عن القيام بها[١].

ولعل هذا الرأي يجد تبريره في أن النقود الإلكترونية (محفظة النقود، برنامج الدفع) عادة ما تصدر بقيمة نقدية صغيرة لمواجهة احتياجات بسيطة للعميل، الأمر الذي لا يتطلب إشراك العميل بقيمة هذه النقود مع جماعة الدائنين والدخول في مفاوضات (فى حالة تقديم البنك طلبا للصلح الواقي من الإفلاس، وما قد يحتاجه ذلك من التفاوض حول إسقاط جزء من الدين، أو منحه أجلا للسداد)[٢]، وإجراءات قد تستغرق وقتا طويلا من شأنها أن ترهق العميل، الأمر الذي يفضل معه تخصيص كفيل لهذا الدين بحيث يحل محل البنك في حالة تعسره للوفاء بالدين.

لكن ماذا لو كانت جماعة الدائنين تتكون من حائزي النقود الإلكترونية فقط، أو كان عددهم كبيرًا وديونهم ذات قيمة كبيرة داخل جماعة الدائنين؟

فى هذه الحالة يكون لحائزي النقود الإلكترونية الدخول في التفليسة بما في حوزتهم من قيم نقدية.

وقد ذهب جانب من الفقه[٣] إلى وجوب تمتع حائزى النقود الإلكترونية في هذه الحالة بحق التقدم على غيرهم من جماعة الدائنين. وقد برر لذلك بأن مقابل إصدار النقود الإلكترونية والذى يحتفظ به البنك لديه، يعد من قبيل التخصيص،

---

(1) **Electronic money**, Report of the working party on electronic money (group of ten): Op. Cit, p. 7.

(٢) لمزيد من التفصيل انظر د. **حسين الماحى**، أحكام الإفلاس في ظل قانون التجارة الجديد، دار النهضة العربية، ٢٠٠٢، ص ٩٠؛ د. **محمد محمد هلالية**، الإفلاس، الطبعة الأولى، ١٤٣١ - ٢٠١٠، (بدون دار نشر)، ص ٢٧٤.

(٣) د. **أحمد السيد لبيب**، المرجع السابق، ص ٢٤٣.

ومن ثم ينحصر حق المطالبة بهذا المقابل على هؤلاء الحائزين فقط.

وعلى الرغم من وجاهة هذا الرأي، إلا أننا لا نتفق معه ويعود ذلك إلى أن الأصل والقاعدة العامة التي تهيمن على مجريات شهر الإفلاس وفقا للنظام القانوني المصري، هي قاعدة المساواة بين جماعة الدائنين في التنفيذ على أموال المدين المفلس، ولا سبيل للخروج على هذه القاعدة إلا باتفاق خاص يقرر منح الدائن حق التقدم على غيره من الدائنين، وهو الأمر الذي لا يتحقق في هذا الفرض. يضاف إلى ذلك أن الغالبية العظمى من معاملات البنك يحتفظ فيها بمقابل لتغطية تنفيذ المعاملة مثل بطاقات الوفاء، ومثل المدخرات التي يتعامل عليها العملاء بأوامر التحويل المختلفة، الأمر الذي لا يجعل لحائزى النقود الإلكترونية خصوصية في هذا الصدد. وبناءً عليه نرى أن يشترك حائزو النقود الإلكترونية في التفليسة في هذه الحالة بوصفهم دائنين عاديين ضمن جماعة الدائنين.

ثانيا- التزامات العميل:

٢٠٨- إصدار النقود الإلكترونية من الخدمات المصرفية التي تقدمها البنوك الإلكترونية لعملائها، وذلك نظير التزام هؤلاء العملاء بدفع المقابل المالي للحصول على هذه الخدمة (والتي تشمل توفير الأدوات والبرامج اللازمة لإجراء عملية الدفع، بالإضافة لشحن أداة الدفع بالوحدات الإلكترونية). ويعد هذا الالتزام الرئيس الذي يقع على عاتق العميل. ويضاف إلى هذا الالتزام بعض الالتزامات التي تحتاج إلى تفصيل على النحو التالي:

١- الالتزام بإعلام البنك الإلكتروني بالبيانات اللازمة للتعاقد:

٢٠٩- سبق أن ذكرنا عند الحديث عن خصائص العقود المصرفية على شبكة الإنترنت أن من أهم الخصائص التي تميز هذه العقود هي كونها تقوم على الاعتبار الشخصي، الأمر الذي يجعل شخصية العميل محل اعتبار من قبل البنك [١]. وعقد الحصول على النقود الإلكترونية لا يخرج عن ذلك، ومن ثم يحرص البنك الإلكتروني على التعرف على شخصية من يطلب خدمة الحصول على النقود الإلكترونية، ولن يتأتى ذلك للبنك إلا من خلال التزام طالب الخدمة بإعلامه بكافة البيانات التي يتطلبها البنك لتقديم هذه الخدمة. سواء تعلقت هذه البيانات بشخص العميل ذاته كاسمه ومحل إقامته وعنوان البريد الإلكتروني الخاص به والرقم القومي الخاص به، أم تعلقت ببيانات عن بعض الضمانات التي قد يتطلبها البنك الإلكتروني لتقديم هذه الخدمة[٢].

ويجب على العميل عند تقديم هذه البيانات أن يتحرى الدقة، وأن يحيط البنك الإلكتروني بكل الظروف التي من شأنها أن تؤدى إلى تغير هذه البيانات[٣]، بحيث يكون هو المسئول عن التبعات المترتبة على وجود خطأ في ذكر هذه البيانات.

هذا ولا يوجد نص في القانون المصري ينظم التزام العميل ومسؤوليته عن الإدلاء بالبيانات الخاصة به للحصول على النقود الإلكترونية، الأمر الذي عالجه

---

(١) راجع سابقا، ص ٣٢٥.

(٢) انظر نموذجًا لعقد الحصول على خدمة النقود الإلكترونية مطلوبًا فيه هذه البيانات على العنوان التالى:

http://www1.uob.com.my/webpages/app_form.htm

(٣) د. أحمد السيد لبيب، المرجع السابق، ص١٨٠.

البنك المركزي كما سبق أن ذكرنا في البند الأول من المسؤوليات الاسترشادية الواقعة على عاتق العميل، والذى قرر من خلاله مسئوليته عن صحة البيانات التي يقوم بإدخالها للبنك عبر شبكة الإنترنت.

هذا ولم يتعرض البنك المركزي لطبيعة البيانات التي يحق للبنك طلبها من العميل للتعاقد، كما لم ينظم مسئولية البنك بخصوصها.

هذا وقد تعرضت عقود تقديم خدمة الدفع بالنقود الإلكترونية لهذا الالتزام، حيث ألزمت العميل بالإدلاء بالبيانات التي يتطلبها البنك أثناء التعاقد، وأعطت للبنك الحق في إنهاء اشتراك العميل ومنعه من استخدام نظام الدفع إذا تبين أن البيانات التي قدمها غير صحيحة(١).

أما عن طبيعة التزام البنك بخصوص البيانات المجمعة من العميل، فالملاحظ أن هذا الأمر يحكمه أمران:

<u>الأول</u>، يتعلق بالحصول فقط على البيانات اللازمة لإصدار النقود الإلكترونية، فلا يتطلب بيانات غير ضرورية في عملية الإصدار. **<u>الثاني</u>**، ويتعلق بالحفاظ على سرية هذه البيانات.

---

(1) **Clause No (3)** if any information you provide is found to be untrue, Cyphermint shall have the right to terminate your use of the System. If you willfully supply false information regarding your identity, you may be subject to federal penalties.
PayCash Terms & Conditions, Eligible users and Reistration information,
http://www.paycashwallet.com/consumer/TermsAndConditions.html

وهذا ما تضمنه التوجيه الأوربي الخاصة بحماية البيانات[١]، حيث عالج الالتزام الأول في المادة السادسة منه، وذلك عن طريق وضع ضوابط معينة يجب على البنك الالتزام بها وهو بصدد تجميعه وتخزينه للبيانات الخاصة بالعميل، وذلك على النحو التالي:

أ- يجب أن يتم تجميع هذه البيانات وفقا لأغراض واضحة ومحددة، وأن يتم التعامل معها وفقا لهذه الأغراض.

ب- يجب أن تكون هذه البيانات كافية وذات صلة بالغرض الذي تم التجميع من أجله، بحيث لا يطلب من العميل بيانات أكثر مما يلزم، وإن حدث هذا يجب حذف البيانات الزائدة.

ج- يجب اتباع إجراءات معينة، وذلك للتأكد من صحة هذه البيانات (كالتوثيق) وضرورتها، والتأكد من أن هذه البيانات سارية حتى تاريخ التعاقد.

د- يجب أن يتم وضع نموذج العقد بطريقة تسمح بتوضيح البيانات المطلوب من العميل ذكرها. ويجب الحفاظ على سلامة هذه البيانات، وذلك من خلال تأمين عملية إدخال هذه البيانات، وكذلك تخزينها.

أما الالتزام الثاني فهو ضرورة الحفاظ على سرية البيانات أثناء تجميعها ومعالجتها[٢]. وقد عبرت المادة السادسة عشرة من التوجيهات سالفة الذكر حيث نص وشدد على وجوب حرص البنك على اختيار الأشخاص الذين يحق لهم تلقي

---

(1) **Directive 95/46/EC,** Official Journal of the European Communities, Article (6).

(2) **Jon M. Peha- Ildar Khamitov**; Op. Cit, p. 3.

هذه البيانات من العملاء وتخزينها(١).

وحسنًا فعل المشرع الأوربي في هذا الصدد، نظرا لأهمية تقيد البنك بهذين القيدين وهو بصدد التعامل مع بيانات العميل. بل يمكن القول بأن هذين القيدين عالقين برقبة البنك حتى في ظل غياب نص صريح من قبل المشرع بذلك، حيث انها أمور يفترض التزام البنك بها وفقا لما تقتضيه طبيعة التعاقدات المصرفية على شبكة الإنترنت. فمثلا على الرغم من أن النظام القانوني المصري يخلو من نص كهذا (التوجيهات الأوربية سالفة الذكر)، إلا أن البنك في ظل أحكام هذا النظام يظل ملتزمًا بألا يحصل من العميل إلا على البيانات اللازمة فقط لإبرام العقد، وبالحفاظ على سرية هذه البيانات. ومن باب أولى أن نقول بأن البنك ملتزم بهذا الالتزام حتى ولو لم يرد النص عليه صراحة في العقد الذي ينظم علاقته بالعميل. فوفقا لنص المادة ١٤٨ من القانون المدني المصري فإن أطراف العقد لا يلتزمون فقط بتنفيذه وفقا لنصوصه، ولكن أيضا بما هو من مستلزماته وفقا لما تقضي به قواعد القانون والعرف والعدالة حسب طبيعة الالتزام.

وبناءً عليه يلتزم البنك دائما بألا يحصل من العميل إلا على البيانات الضرورية، وبالحفاظ على سرية هذه البيانات. وذلك بمناسبة إبرامه عقد الحصول على خدمة الدفع الإلكتروني من البنك. لكن هذه ليست دعوة لاحتفاظ المشرع المصري بموقفه هذا، حيث إن دور النص القانوني لا يقتصر فقط على مجرد الإلزام بمضمونه، ولكن أيضا وضع تنظيم واضح ومحدد للأمر محل التنظيم، خاصة إذا ما اتصل الأمر بموضوع حديث النشأة كالعمليات المصرفية

---

(1) **Directive EC, 95/46/**, Official Journal of the European Communities, Article (16).

على شبكة الإنترنت، وذلك على النحو الذي عرضت له التوجيهات الأوربية سالفة الذكر.

لكن التساؤل يثور بخصوص طبيعة المعلومات التي يطلب البنك من العميل الإدلاء بها وهو بصدد التعاقد معه للحصول على خدمة الدفع الإلكتروني.

يمكن القول بإنه في إطار التزام البنك بالإفصاح عن كافة الخطوات التي يجب على العميل اتباعها للحصول على الخدمة، بالتزام الأول بتحديد طبيعة البيانات التي يجب على الثاني تقديمها أثناء التعاقد، وسبب تطلبه لهذه المعلومات، وأمثلة لهذه المعلومات[١]:

أ- المعلومات التي من شأنها التعريف بشخصية العميل (مثل الاسم، العنوان، رقم الهاتف، رقم التأمين الاجتماعي "social Security number").

ب-البيانات الخاصة بحساب هذا العميل، أو نماذج القروض (Loan application) التي حصل عليها من البنك، وغيرها من البيانات الخاصة بتعاملات هذا العميل المالية مع البنك.

ج- معلومات خاصة بصفقات سبق القيام بها، وعمليات الدفع المرتبطة بها، وبيان إذا ما كان هناك حالات سحب بدون رصيد (overdraft) قد تمت من عدمه.

---

(١) انظر نموذجًا لهذه البيانات المعلنة على موقع أحد البنوك الإلكترونية العاملة عبر شبكة الانترنت.

NetBank, privacy policy at NetBank, available at: http://www.netbank.com/about_privacy.htm

د- معلومات من التقارير الخاصة بتعاملات العميل مع المؤسسات المالية تفيد أهليته (Eligibility) للحصول على خدمات الائتمان، والتعاملات المالية، وهذه المعلومات مثل معدل الائتمان الممنوح له، وتوازن حسابه (الدائن والمدين) والمبالغ المستحقة عليه.

ه- المعلومات الخاصة بتعاملاته مع البنك عبر شبكة الإنترنت، مثل رقم التعريف الشخصي له (PIN)، وكلمة المرور(password) الخاصة به.

ويجب أن تكون مسئولية البنك في خصوص الحفاظ على سرية هذه البيانات مسئولية مشددة، بأن يكون التزامًا بتحقيق نتيجة، وأن يسأل البنك شخصيا عن ذلك؛ كما في حالة انتهاك سرية هذه البيانات بسبب وجود تقصير في النظم الأمنية المسئولة عن الحفاظ على هذه البيانات. وفي هذه الحالة لا يكون العميل مكلفًا بإثبات هذا التقصير من قبل البنك، بل يكفيه فقط إثبات عدم تحقق النتيجة المرجوة، بحدوث انتهاك لسرية بياناته. ولا يستطيع البنك لدفع مسؤوليته في هذه الحالة إثبات قيامه بالاحتياطات الكافية لمنع هذا الانتهاك، بل يحتاج إلى إثبات السبب الأجنبي.

كما يسأل البنك عن انتهاكات العاملين لديه، وذلك بوصفه متبوعا، ما دام ثبت وقوع هذا الإخلال من أحد العاملين لديه، وكان ذلك أثناء أو بسبب قيامه بمهام عمله لدى البنك. وعلى العميل إثبات عناصر هذه المسؤولية. ولا يستطيع البنك دفع مسؤوليته بإثبات انتفاء الخطأ أو انقطاع علاقة السببية بين الخطأ والضرر، بل عليه إثبات السبب الأجنبي وذلك تطبيقا لحكم المادة ١٧٤ من

القانون المدني المصري[1].

٢- الالتزام باستخدام نظام النقد الإلكتروني استخداما سليما:

٢١٠- يأتي في مقدمة التزامات العميل في مواجهة البنك المصدر للنقد الإلكتروني استخدام هذا النقد استخداما سليما. ويتحقق هذا الالتزام من قبل العميل بمراعاة أمرين:

الأول: المحافظة على أداة الدفع سواء تمثلت في بطاقة ذكية أم محفظة افتراضية، وما يرتبط باستخدام هذه الأداة من بيانات كاسم المستخدم، ورقم التعريف الشخصي الخاص به (PIN)، وذلك من خلال الحيلولة دون استعمالها من قبل الغير بأي شكل من الأشكال[2]. فاستعمال أداة الدفع أمر شخصي بالنسبة لصاحبه، كما أن البيانات المرتبطة باستعمال هذه الأداة، سرية ويجب أن يحتفظ بها بشكل آمن، وعدم السماح للغير بالاطلاع عليها أو المشاركة في استعماله[3].

الثاني: استعمال نظام النقد الإلكتروني استعمالا صحيحا، وذلك من خلال امتثال العميل للنظام الذي رسمه له البنك لاستعمال نظام النقد. وهذا النظام يشتمل على

(١) **المادة ١٧٤ من القانون المدني** " يكون المتبوع مسئولا عن الضرر الذى يحدثه تابعه بعمله غير المشروع، متى كان واقعا منه في حال تأدية وظيفته أو بسببها".

(2) **James E Backhouse**; Op. Cit, p. 30.

(٣) د. **أحمد السيد لبيب**، المرجع السابق، ص١٨٢؛

Paragraph (11) you agree to protect the confidentiality of your accounts and account number, your user ID and password and the security codes.

United overseas bank, E-statement service Application form, Terms and conditions, Available at : http://www1.uob.com.my/webpages/app_form.htm

البنود والالتزامات الواردة في العقد الذي يحكم العلاقة بينه وبين البنك، وكذلك التعليمات التي يوصى بها البنك عميله في هذا الخصوص[١]. فالبنك ملتزم في مواجهة العميل بتمكينه من استعمال أداة الدفع، ليس فقط من خلال تسليمه هذه الأداة، ولكن أيضا من خلال تزويده بكافة التعليمات والإرشادات التي سوف يسير على هديها لاستعمال هذه الأداة وفي المقابل يلتزم العميل باتباع هذه التعليمات من أجل تحقيق أقصى استفادة من نظام النقد، وتجنب أي مشاكل تحدث في هذا الخصوص. وهذه التعليمات مثل الخطوات الشارحة لكيفية تشغيل أداة الدفع، والتحذيرات المتعلقة باستعمالها أو الاحتفاظ بها في أماكن معينة، كذلك التعليمات الواجب اتباعها في حالة فقد أداة الدفع، أيضا أسماء التجار المتعاقد معهم البنك لقبول الدفع بهذه الأداة.

هذا ولم يرد نص في القانون المصري ينظم التزام العميل باستخدام نظام النقد استخداما سليما، الأمر الذي تداركه التوجيه الرابع الصادر عن البنك المركزي في مالطا، والخاص بإصدار النقود الإلكترونية، من ضرورة التزام العميل بالمحافظة على أداة الدفع الإلكتروني، الدفع، والوسائل المرتبطة بها، مثل رقم التعريف الشخصي الخاص باستعمال أداة الدفع، وعدم كتابته بطريقة سهلة التمييز عند استعمال أداة الدفع لإجراء إحدى الصفقات، وذلك من خلال اتخاذ كافة الخطوات اللازمة لذلك في ضوء العقد الذي يحكم العلاقة بينهما[٢].

---

(١) د. شريف محمد غنام، محفظة النقود الالكترونية، المرجع السابق، ص١٤٦.

(2) (a) use the electronic payment instrument in accordance with the terms governing the issuing and use of a payment instrument; in particular, the holder shall take all reasonable steps to keep safe the electronic payment instrument and the means (such as

وتجدر الإشارة إلى أهمية هذا الالتزام بالمعنى السابق بالنسبة للبنك الإلكتروني؛ وذلك لتوقف نجاح عملية الدفع برمتها على حسن استعمال نظام النقد من قبل العميل. يضاف إلى ذلك أن البنك يظل محتفظا بملكية أداة الدفع طوال فترة التعاقد، على أن يردها العميل له عند نهاية العقد، الأمر الذي سيكون دافعا للبنك للتشديد من التزام العميل باستخدام نظام النقد استخداما سليما، بأن يجعله التزاما بتحقيق نتيجة بحيث تنعقد مسئولية العميل عن أي تلف يلحق هذه الأداة، دون أن يكون البنك مكلفا بإثبات خطأ العميل في ذلك، مادام أنه سلمه أداة الدفع وهي في حالة جيدة، وزوده بكافة التعليمات اللازمة لاستعمالها. ومسؤولية العميل في هذه الحالة لن تكون مقصورة على التلف أو فقد أداة الدفع، ولكن أيضا يكون مسئولا عن الأضرار المتعلقة بالاستعمال غير المشروع لهذه الأداة خلال الفترة السابقة على إبلاغ البنك بهذا الفقد. ولا يستطيع العميل أن يدفع مسؤوليته في هذه الحالة إلا بإثبات السبب الأجنبي.

٣- إعادة أداة الدفع للبنك الإلكتروني عند انتهاء التعاقد:

٢١١- تظل أداة الدفع التي يقوم البنك الإلكتروني بتسليمها للعميل ملكا للأول على نحو يفرض على الثاني التزاما بإعادتها عند انتهاء العلاقة التعاقدية التي تربط بينهما، الأمر الذي يبرر تشديد البنك من التزام العميل بالمحافظة على هذه

---

a personal identification number or other code)

(c) "not record his personal identification number or other code in any easily recognisable form, in particular on the electronic payment instrument or on any item which he keeps or carries with the electronic payment instrument".

Central bank of Malta, Directive No 4, electronic payment services, Op, Cit, p. 4.

الأداة واستخدامها استخداما سليما، بل ويفسر طبيعة المقابل الذي يقــوم العميــل بدفعه للبنك عند حصوله على هذه الأداة؛ فهو ليس ثمنا يدفع نظير الحصول على هذه الأداة، بل هو مقابل للانتفاع بها من خلال استعمالها في عمليات الدفع، على أن تبقى للبنك ملكية الأداة. بل أن هذا ما قد يبرر لنا بعض التصرفات المتشددة التي قد يقوم بها البنك في مواجهة العميل؛ كقيامه بإلغاء أداة الدفع، أو سحبها من العميل دون إخطار مسبق، وبدون إبداء أسباب(١).

ويلتزم العميل بهذا الالتزام سواء كانت نهاية العقد طبيعية بانتهاء مدتــه أم كانت نهاية مبتسرة بالفسخ أو غلق الحساب أو غير ذلك من الأسباب. وتلتــزم جهة الإصدار في هذه الحالة بإعادة كافة المبالغ التي توجد فــي حــساب النقــد الإلكتروني الخاص بالعميل إليه بالإضافة إلى المبالغ التي تحتويهــا أداة الــدفع ذاتها عند غلق الحساب أو انتهاء العقد(٢).

---

(١) انظر في خصوص تمتع جهة الإصدار بالحق في إنهاء الخدمة وإلغاء أداة الدفع بدون ذكر أسباب ودون سبق إخطار بذلك عقد "Netcash ":

Net Cash Terms of Use, Suspension/Termination: (Net Cash reserves the right, without notice and in its sole discretion, to terminate your license to use the Net Cash Site, and to block or prevent your future access to and use of the Services for any reason whatsoever).**Net Cash Terms of Use,** Your Representations/Warranties, available at: https://www.netcash.com/engine/show?topic=terms

- هذا وإن كنا نتحفظ كثيرا على إطلاق يد البنك في إلغاء أداة الــدفع وســحبها مــن العميل بدون ذكر أسباب، حيث إن هذا الفعل يشكل إهدارًا شديدا لحــق العميــل كطرف ثان في عقد إصدار النقود الإلكترونية، ويعكس إجحافا كبيرا من قبل البنك بحقه في مجرد معرفة أسباب الإلغاء. فحتى في الحالات التي يتجاوز فيها العميل حدود الاستعمال المشروع لأداة الدفع، يجب أن يخطره البنك بالإلغاء وأسبابه.

(٢) د. أحمد السيد لبيب، المرجع السابق، ص١٨٥.

ولم ينظم هذا الالتزام من قبل المشرع المصري، أيضا لم تتعرض القوانين والتوجيهات الأوربية لتنظيم هذا الالتزام، لكن تواترت عقود إصدار النقود الإلكترونية على تنظيمه كأحد الشروط العقدية (١)، ومن ثم فهو التزام عقدي، يستمد تنظيمه والزاميته من واقع العقد. ويترتب على مخالفته من قبل العميل انعقاد مسؤوليته العقدية عن عدم قيامه برد أداة الدفع، أو ردها وهي تالفة غير صالحة للاستعمال (وذلك باعتباره مسئولاً عن حسن استعمالها) بعد نهاية العقد.

بل يمكن القول بمساءلة العميل جنائيا عن جريمة خيانة الأمانة إذا لم يقم برد أداة الدفع للبنك، وذلك إذا تضمن العقد ما يفيد تسليم هذه الأداة له على سبيل الأمانة (كما لو نص البنك على أن العميل تسلم أداة الدفع على سبيل الإيجار)، وذلك وفقا لحكم المادة ٣٤١ من قانون العقوبات المصري.

ثالثا- التزامات التاجر:

٢١٢- يقع على عاتق التاجر الذي ينضم إلى نظام الدفع الإلكتروني عدة التزامات، أهمها الالتزام بقبول الدفع بالنقود الإلكترونية من قبل العميل، والتأكد من صحة عملية الدفع، والمحافظة على سرية البيانات الخاصة بالعميل وذلك على التفصيل التالي:

---

(١) وهذا الالتزام يفرض أيضا على حاملي بطاقات الائتمان. انظر المادة الثامنة من شروط إصدار بطاقة ماستر كارد البنك التجاري الدولي **CIB** والتي تنص على أن "تعتبر البطاقة ملكا للبنك ويتعين على حامل البطاقة أن يردها بمجرد طلبها، ويجوز لحامل البطاقة في أي وقت أن ينهى الاتفاق بينه وبين البنك بناء على طلب كتابي منه بإلغاء البطاقة، ويتعين عليه إعادة البطاقة، ويجوز للبنك إلغاء البطاقة أو سحبها في أي وقت بدون إشعار مسبق كما يجوز رفض إعادة إصدارها أو تجديدها دون إبداء الأسباب وذلك كله دون الإخلال بحق البنك بالخصم من حساب العميل بالمديونيات الناشئة عن استخدام البطاقة وحتى تاريخ إعادتها للبنك أو الإخطار الكتابي".

١- الالتزام بقبول الوفاء بالنقود الإلكترونية:

٢١٣- من أولى الالتزامات التي تقع على عاتق التاجر المنضم لنظام الدفع الإلكتروني هو قبول الوفاء بالنقود الإلكترونية من قبل حائز هذه النقود(١)، وهذا الالتزام يبرز خصوصية النقود الإلكترونية في مواجهة النقود التقليدية؛ حيث إن الأخيرة مقبولة من قبل الكافة، على عكس النقود الإلكترونية المقبولة فقط من قبل التجار المتعاقدين مع البنك على قبول الوفاء بها. ومرجع هذه التفرقة هو مصدر قوة الإبراء التي يتمتع بها كل نوع من هذه النقود، حيث إن مصدر هذه القوة في النقود التقليدية هو القانون(٢)، أما في النقود الإلكترونية فمصدر الإلزام هو اتفاق المتعاقدين، الأمر الذي يلقى على عاتق البنك زيادة التعاقد مع أكبر عدد من التجار، من أجل توسيع رقعة قبول هذه النقود في الوفاء، بما سيؤدى إلى جذب المزيد من العملاء.

هذا ولم يعالج المشرع المصري هذا الالتزام، كما لم يظهر معالجته من قبل النظم القانونية الأخرى.

ويجب على البنك قبل أن يفرض هذا الالتزام على التاجر بموجب العقد الذي يجمع بينهما، وأن يزوده بكافة الأجهزة والبرامج التي تمكنه من قبول الوفاء بالنقود الإلكترونية. كما يجب على العميل أن يقوم باستعمال أداة الدفع في مواجهة التاجر استعمالا سليما وفقا للتعليمات الموضوعة من قبل البنك لهذا الغرض، بحيث يمكن القول بتحمل التاجر المسؤولية كاملة بعد ذلك عن

---

(1) **Andres Guadamuz**; Op, Cit, p. 2.

(٢) المادة ١٠٨ من قانون البنك المركزي ٨٨ لسنة ٢٠٠٣. "يكون لأوراق النقد التي يصدرها البنك المركزي قوة إبراء غير محدودة ".

الأضرار التي تلحق بالعميل والبنك من بعده (حيث يضار البنك في سمعته) نتيجة عدم قبوله الوفاء بالنقود الإلكترونية من قبل حائزها الشرعي. فالعميل يستطيع في هذه الحالة الرجوع مباشرة على البنك بموجب أحكام المسؤولية العقدية، حيث يكفيه لذلك إثبات عدم تحقق النتيجة المرجوة من التعاقد (الوفاء الإلكتروني) دون أن يكون مكلف بإثبات خطأ البنك في ذلك. ولا يستطيع الأخير دفع مسؤوليته في هذه الحالة إلا بإثبات السبب الأجنبي.

كما يستطيع البنك بعد ذلك الرجوع مباشرة على التاجر بأحكام المسؤولية العقدية، وذلك بموجب العقد الذي يجمع بينهما. كما لا يستطيع التاجر أيضا دفع مسؤوليته في مواجهة البنك إلا بإثبات السبب الأجنبي.

لكن ماذا لو كان السبب في عدم تحقق عملية الوفاء لا يعود لخطأ التاجر، بل يعود لسوء عمل أدوات الوفاء التي زوده البنك بها؟

هنا يمكن القول بعدم مسئولية التاجر عن عدم الوفاء في هذه الحالة، وذلك مادام أنه اتخذ كافة الاحتياطات اللازمة لإتمام عملية الوفاء، ولكنها لم تتحقق بسبب سوء عمل الأجهزة التي زوده البنك بها.

ويمكن القول بأن العميل يجد ضالته المنشودة في هذه الحالة في نظرية المخاطر (تحمل التبعة)(١) التي تمكنه من الرجوع على البنك حتى لو ثبت عدم

---

(١) هذا وقد وجدت نظرية تحمل التبعة تطبيقا قضائيا لها في مجال المعاملات المصرفية؛ حيث قضت محكمة النقض المصرية بمسؤولية البنك عن الأضرار التي لحقت بعميله نتيجة قيام البنك بصرف شيك مزور من حساب العميل، وقد أكدت المحكمة عدم ثبوت خطأ من قبل البنك، ولكن مسؤليته تأسست على الضرر الذى لحق العميل. راجع **نقض مدني مصري**، ١٩٦٦/١/١١، س ١٧، قاعدة (١٢)، مجموعة أحكام محكمة النقض، ص ١٩٤.

وجود خطا من جانب الأخير. فيكفى العميل في هذه الحالة إثبات الضرر الذي لحقه من جراء عدم تحقق الوفاء، وإثبات علاقة السببية بين نشاط البنك وتحقق هذا الضرر حتى تنعقد مسؤوليته عن هذه الأضرار. ولا يستطيع البنك دفع مسؤوليته في هذه الحالة إلا بإثبات السبب الأجنبي، كوجود قوة قاهرة حالت دون تحقق عملية الدفع(١). ويمكن القول بإن البنك في هذه الحالة لن يملك الرجوع على التاجر؛ وذلك لأنه المسئول عن تزويد التاجر بالأجهزة والبرامج اللازمة لعملية الوفاء. وهذا التشديد الواضح في مسئولية البنك تفرض عليه مزيدا من الحرص والتدقيق عند انتقاء الأجهزة والبرامج التي تتم عملية الدفع من خلالها، بل تدفعه إلى مراجعة أداء عمل هذه الأجهزة بصورة دورية لضمان سلامة عملية الدفع.

وفي النهاية يجب أن نفرق بين رفض التاجر الوفاء بالنقود الإلكترونية، وبين رفضه التعامل مع العميل. فالحالة الأولى يكون الرفض فيها موجها لوسيلة الدفع (النقود الإلكترونية)، ومن ثم تنعقد مسئولية التاجر على النحو السابق. أما في الحالة الثانية يكون للتاجر مطلق الحرية في أن يتعامل مع العميل من عدمه، فقد تكون شروط العميل غير مرضية، ففي هذه الحالة من حقه رفض التعامل مع العميل حتى ولو كان بحوزته نقود إلكترونية(٢).

٢- الالتزام بالتأكد من سلامة النقود الإلكترونية:

٢١٤- باعتبار أن عملية الوفاء بالنقد الإلكتروني هي من أهم المراحل في نظام

---

(١) د. **شريف محمد غنام**، مسؤولية البنك عن أخطاء الكمبيوتر في النقل الإلكتروني للنقود،مرجع سابق، ص١٠٥.

(٢) د. **شريف محمد غنام**، محفظة النقود الإلكترونية، مرجع السابق، ص١٥٣.

عمل النقود الإلكترونية، وذلك بالنظر إلى أنها مرحلة جني الثمار، فكان من الضروري إلزام التاجر (باعتباره أحد أفراد منظومة الدفع) بالتأكد من سلامة وصلاحية الدفع بهذه النقود، سواء من ناحية سلامة وسيلة الدفع الإلكتروني، أم من ناحية سلامة وحدات النقد الإلكتروني المشحونة بها.

هذا ولم يرد نص في النظام القانوني المصري يعالج التزام التاجر بالتأكد من سلامة النقود الإلكترونية التي يقوم العميل بدفعها.

لكن وجد هذا الالتزام حرصا من قبل المجلس الأمريكي للرقابة على المؤسسات، حيث ذهب إلى التزام التاجر بالتأكد من سلامة وصلاحية الدفع بالنقود التي في حوزة العميل(١).

وتجدر الإشارة إلى أن التزام التاجر بالتأكد من سلامة النقود الإلكترونية ينصرف إلى صلاحية النقود الإلكترونية للاستعمال، دون أن يتطرق إلى التأكد من شخصية القائم بالدفع أو ملاءته(٢).

ويستطيع التاجر القيام بذلك على مرحلتين: الأولى، وفيها يتأكد من سلامة وسيلة الدفع الإلكتروني، وذلك من خلال التحقق من أن أداة الدفع الإلكتروني

---

(1) **Interagency council issues guidance on electronic financial services and consumer compliance**, Federal financial institutions examination council; Op. Cit, p. 3.

(٢) وفي هذا تختلف النقود الإلكترونية عن بطاقات الائتمان، حيث يجب على التاجر في بطاقات الائتمان التأكد من شخصية القائم بالدفع أو ملاءته؛ حيث إن هذه أمور ليست محل اعتبار في حالة الدفع بالنقود الإلكترونية، والسبب في ذلك أن النقود الإلكترونية شأنها شأن النقود التقليدية تتميز بأنها غير اسمية، فهي لا تحمل بيانات خاصة بحاملها ولا ترتبط بحساب مصرفي، لذلك يقبلها التجار دون حاجة إلى تحديد شخصية القائم بالدفع. د.**أحمد السيد لبيب**،المرجع السابق، ص١٨٧.

ليست ضمن الأدوات الضائعة أو المسروقة أو المزورة التي أخطره بها البنك الإلكتروني[1]. ويمكن له ذلك من خلال التأكد من هوية حائز أداة الدفع، عن طريق النظر في رقم الأداة (والذي يكون مسجلا عليها)، والتوقيع الإلكتروني الخاص بحائز هذه الأداة[2].

والمرحلة الثانية، وهي التي يتم فيها التأكد من صلاحية وحدات النقد الإلكتروني، وذلك من خلال اتصال التاجر بقاعدة البيانات الخاصة بالبنك الإلكتروني، والتي يحتفظ فيها بكل الأرقام المسلسلة الخاصة بوحدات النقد الإلكتروني التي سبق إنفاقها، فإذا وجد أن هذه الوحدات لم يسبق إدراجها من قبل العميل في تلك القاعدة، فعليه أن يقبلها في الوفاء فهذا يعنى أنها نقود صحيحة. أما إذا وجد سبق إدراجها من قبل العميل فعليه الامتناع عن قبول الوفاء بهذه النقود[3].

والسؤال: ماذا لو قبل التاجر الوفاء بنقود إلكترونية غير صالحة للاستعمال؟

يمكن القول بضرورة التفرقة في هذه الحالة بين أمرين:

الأول: إذا كان قبول الوفاء قد تم قبل إخطاره بعدم صلاحية هذه النقود للاستعمال، حيث لا مسئولية عليه في هذه الحالة، مادام أنه اتبع كافة الإجراءات والتعليمات الخاصة بقبول الوفاء بأداة الدفع، بأن تأكد من عدم درج أداة الدفع

(1) **Interagency council issues guidance on electronic financial services and consumer compliance**, Federal Financial Institutions Examination Council; Op. Cit, p. 3.

(٢) **د. شريف محمد غنام**، محفظة النقود الالكترونية، المرجع السابق، ص١٥٤.

(3) **Andres Guadamuz**; Op, Cit, p. 3

لديه ضمن الأدوات المسروقة، ومن صلاحية الوحدات الإلكترونية لعدم سبق إنفاقها. ويجب على البنك أن يقبل طلبه بتحويل الوحدات الإلكترونية التي في حوزته إلى نقود عادية، على أن يتحمل المسؤولية بعد ذلك من أخل في القيام بالإخطار، سواء كان العميل أم البنك.

الثاني: إذا كان قبول الوفاء قد تم بعد إخطاره بعدم صلاحية هذه النقود للاستعمال. هنا يتحمل التاجر المسؤولية كاملة، حيث إن قبوله الوفاء رغم إخطاره ينم عن إهماله في اتخاذ الإجراءات اللازمة للتأكد من صلاحية هذه النقود للوفاء. ومن ثم يحق للبنك في هذه الحالة ألا يقبل طلبه بتحويل هذه الوحدات إلى نقود عادية.

بل يمكن أن نذهب إلى أبعد من هذا بالقول بأن التاجر لو قبل الدفع بالنقود الإلكترونية وهو يعلم أنها مزورة أو مسروقة، وقام على الرغم من ذلك بطلب تحويلها إلى نقود عادية من البنك بمسئوليته عن جريمة النصب، وذلك وفقا لنص المادة ٣٣٦ من قانون العقوبات المصري(١).

٣- الالتزام بالحفاظ على سرية البيانات الخاصة بالعميل:

٢١٥- يجب أن يلتزم التاجر بالتزام عام في مواجهة كل من البنك الإلكتروني

---

(١) تنص المادة ٣٣٦ من قانون العقوبات المصري على " يعاقب بالحبس كل من توصل إلى الاستيلاء على نقود أو عروض أو سندات دين أو سندات مخالصة، أو أي متاع منقول، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها، أما باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة أو إحداث الأمل بحصول ربح وهمي أو تسديد المبلغ الذي أخذ بطريقة الاحتيال أو إيهامهم بوجود سند دين غير صحيح أو سند مخالصة مزور وإما بالتصرف في مال ثابت أو منقول ليس ملكا له وليس له حق التصرف فيه، وإما باتخاذ اسم كاذب أو صفة غير صحيحة. أما من شرع في النصب ولم يتممه فيعاقب بالحبس مدة لا تتجاوز سنة".

والعميل بالحفاظ على سرية البيانات التي قد تصل إلى علمه بمناسبة التعاملات التي يجريها العميل معه باستخدام أداة الدفع. فاستخدام هذه الأداة يترتب عليها قيام العميل بالإفصاح عن بعض البيانات الخاصة به كاسم المستخدم والرقم السري على صفحة الويب الخاصة بالتاجر الذي يتعامل معه، بل لا يقتصر الأمر فقط عند حد الإفصاح، بل يتطرق لما هو أبعد من ذلك وهو عدم مراقبة سلوكيات العميل الخاصة باستخدام هذه الأداة؛ حيث إن سلوكيات العميل في هذا الخصوص قد تتحدث بصورة غير مباشرة عن هويته[١]، الأمر الذي يفرض على التاجر ضرورة الحفاظ على سرية هذه البيانات. ويتحقق ذلك من جانب التاجر ليس فقط من خلال التكتم على كل ما يصل إلى علمه من بيانات، بل أيضا من خلال التسلح بنظم إلكترونية تكفل أمن وسلامة هذه البيانات عند قيام العميل بالدفع في مواجهته.

هذا وقد أكدت المسؤوليات الاسترشادية الصادرة عن البنك المركزي المصري على هذا الالتزام[٢]، حيث جاء في البند الرابع: (في حالة وجود طرف آخر تقدم من خلاله الخدمة، يتعين على مجلس إدارة البنك إقرار اتفاقية التشغيل التي تنظم العلاقة بين البنك مع هذا الطرف وتحديد مسئوليته في الحفاظ على سرية التعليمات والمعاملات التي تتم عبر الشبكات وأية معلومات تتاح له).

وحسنا فعل البنك المركزي في هذا الخصوص، وإن كانت أهمية الأمر تدعو إلى ضرورة تصدى المشرع المصري بنص صريح يعالجه، ولا يكتفي

---

(1) **Gennady Medvinsky, B.Clifford Neuman** ; Op, Cit, p. 1.

(٢) الضوابط الرقابية للعمليات المصرفية الإلكترونية وإصدار وسائل دفع للنقود الإلكترونية، مرجع سابق، ص١٠.

بمجرد توصيات تصدر عن البنك المركزي تعالج الأمر بصورة عامة.

وإلى أن يتم التدخل من قبل المشرع، يجب على البنك أن يشدد من مسئولية التاجر في هذا الخصوص، وذلك من خلال النص على هذا الالتزام صراحة في العقد الذي يحكم العلاقة بينهما، وأن يجعل التزام التاجر بذلك التزاما بتحقيق نتيجة وليس ببذل عناية، بحيث تنعقد مسؤوليته بمجرد حدوث إفشاء لسرية هذه البيانات، ودون أن يكون العميل مكلفًا بإثبات خطأ التاجر، باعتبار أنه أمر مفترض في حق التاجر لمجرد حدوث الضرر. ويبرر تشديد مسئولية التاجر في هذا الخصوص بطبيعة البيئة المفتوحة التي يتم فيها استخدام أداة الدفع الإلكتروني، ومن ثم إفشاء البيانات المرتبطة بهذا الاستخدام، حيث يشكل الالتزام بالسرية أهمية خاصة في هذا المجال.

وبعد الانتهاء من عرض لأهم الجوانب الخاصة بإصدار النقود الإلكترونية كأحد أهم صور العمليات المصرفية التي يتطلع لها البنك الإلكتروني العامل عبر شبكة الإنترنت، لا يسعنا إلا أن نوجه النداء للمشروع المصري الذي طال ثباته، وذلك بضرورة التدخل العاجل بنصوص صريحة لمعالجة هذه الجوانب من نظام عمل هذه النقود، وذلك من أجل وضع ضوابط محددة لحق البنك في إصدار مثل هذه النقود، ورسم حدود واضحة لالتزامات ومسؤوليات أطراف هذه العملية، وذلك على نحو يراعى فيه طبيعة عمل البنك وطبيعة البيئة التي يعمل فيها، ويراعى أيضا ظروف العميل كطرف ضعيف في هذه العلاقة، يحتاج إلى تنظيم قانوني يحقق له الإنصاف في الحالات التي يتجاوز فيها البنك حدود المعقول وهو بصدد صياغة العقود التي تحكم تقديمه لهذه الخدمة، بل لا نكون قد تجاوزنا إذا ما وصل بنا الطلب إلى حد إكساب المشرع لهذه النقود قوة إبراء قانونية،

وذلك على النحو الذي يجعلها مقبولة كوسيلة للوفاء من قبل الكافة، مع وضـــعه الضوابط اللازمة لذلك.

المبحث الثاني

التحويل المصرفي الإلكتروني للنقود

٢١٦- يُعد التحويل المصرفي للنقود[١] من أهم وأخطر الموضوعات المؤثرة في حركة التجارة على الصعيدين الوطني والدولي، وذلك لما تتمتع به هذه العملية من قدرة فائقة على تسوية المدفوعات فيما بين الأفراد عن طريق البنوك بشكل أمن وميسر. وقد كانت هذه العملية تقوم فيما مضى على المراسلات الورقية، والتي كانت تقوم على التبادل الأصم للبيانات والمعلومات والتحليلات والأرقام الإحصائية والمحاسبية فيما بين البنوك.

ومع حدوث تطور في وسائل الاتصال (كالتلغراف) أخذت البنوك في تسخير هذه الوسائل كي تلبى احتياجاتها من إتمام عمليات التحويل بشكل أسرع وأوفر في التكلفة. وقد واصلت عجلة التطور دورانها إلى أن وصل الحال إلى حدوث تزاوج بين نظم الاتصالات والمعلومات الحديثة من ناحية ونظم الحواسيب من ناحية آخري، الأمر الذي نتج عنه ميلاد البنك الإلكتروني على شبكة الإنترنت، بما أحدث طفرة في نظم تسوية المدفوعات الخاصة بالصفقات التجارية، والتي يأتي على رأسها التحويلات النقدية[٢]، وهذه الطفرة لم تكن

---

(١) **وقد عرف المشرع المصري في قانون التجارة رقم ١٧ لسنة ١٩٩٩ في المادة ٣٢٩ الفقرة الأولى** التحويل المصرفي بأنه عملية يقيد البنك بمقتضاها مبلغا معينا في الجانب المدين من حساب الآمر بالتحويل بناء على أمر كتابي منه وفي الجانب الدائن من حساب آخر.

(٢) رأسم **سميح محمد عبد الرحيم**، مرجع سابق، ص١٠٣؛

Charles A. Oswald, A comparative Historical, Legal and policy

بمضمون هذه النظم، بل كانت في أسلوب إجرائها.

٢١٧- وتلعب البنوك العاملة على شبكة الإنترنت دورا محوريا في عمليات التحويل الإلكتروني للنقود[١]، هذا الدور الذي ظهر أثره ليس في مجرد تطويع هذه البنوك لشبكة الإنترنت للاتصال فيما بينها لإتمام عمليات التحويل، ولكن أيضا في اتصال عملائها بها من خلال أشكال متعددة (بطاقات السحب النقدي ATM، البريد الإلكتروني، الشيكات الإلكترونية)، وذلك لإجراء عملية التحويل الإلكتروني للنقود[٢].

ونظرا لاحتلال هذه العملية أهمية كبيرة في نظام عمل البنك الإلكتروني؛ وذلك بالنظر لدورها الكبير في حركة التجارة، فإن الأمر يستدعي أن نتعرف على ماهية هذه العملية كإحدى العمليات المصرفية للبنك، وذلك من حيث تعريفها، وإبراز أهم خصائصها،وكيفية إجراؤها على شبكة الإنترنت. (مطلب أول)، ثم لالتزامات أطراف عملية التحويل، والمسؤوليات المترتبة على ذلك (مطلب ثاني).

---

analysis of informal and formal money Transfer systems, dissertation presented to school of law, saint Thomas university, December 2007, p. 45.

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 32.

(2) **Electronic fund transfers**, Consumer handbook to credit protection laws, The federal reserve board, August 2007, p. 2; **consumer rights in electronic fund transfers**, California department of consumer affairs division of legal affairs (Legal Guide CR-6), May 2003, p1.

المطلب الأول

ماهية التحويل الإلكتروني للنقود

كإحدى العمليات المصرفية على شبكة الإنترنت

٢- يعرف التحويل المصرفي للنقود بصورة عامة بأنه عبارة عن نقل مبلغ معين من حساب شخص يسمى الآمر بناء على طلبه المكتوب، وقيد هذا الجانب الدائن لحساب شخص آخر يسمى المستفيد (قد يكون الآمر أو شخصًا آخر)، وذلك في ذات البنك أو في بنك آخر[١].

ويعكس هذا التعريف شروط التحويل المصرفي وهي:

أ - وجود حسابين.

ب- ورود التحويل على مبلغ نقدي محدد.

ج- صدور أمر بالتحويل.

وفي ضوء ذلك، يمكن القول بأن عملية التحويل المصرفي للنقود هي من العمليات التي لا يمكن إجراؤها إلا بمعرفة بنك. فهذه العملية أيا ما كانت أطرافها، وأيا ما كانت الوسائل المستخدمة لإجرائها، فلابد لها من بنك يقوم على تنفيذها. وعملية التحويل بهذا المعنى تختلف عن عملية تبادل البيانات الخاصة بعملية التحويل: فالأولى هي عبارة عن نقل مبلغ معين من حساب مصرفي إلى

---

(١) د. **على جمال الدين عوض**، مرجع سابق، ص ١٢٩.

حساب آخر. أما الثانية فهي عبارة عن نقل المعلومات المتعلقة بهذا التحويل[١]،

ولتوضيح المعنى أكثر نفترض أن شخصا قام بإجراء صفقة تجارية ترتب عليها أن أصبح مدينا بمبلغ معين لمن أجرى معه هذه الصفقة، وعلى أثر ذلك قام بتحرير شيك بهذا المبلغ، وسلم هذا الشيك إلى الدائن، هنا يعد تسليم الشيك نقلا للبيانات الخاصة بعملية التحويل. أما قيام البنك على أثر وصول هذا الشيك لديه بنقل قيمته من حساب المدين إلى حساب الدائن فهذا ما يمكن أن نطلق عليه التحويل المصرفي للنقود.

والتحويل المصرفي للنقود بهذا المعنى ينطوي على قيد مزدوج، الأول بالخصم من حساب الآمر بالتحويل، والثاني بالإضافة في حساب المستفيد. وتنقسم عملية التحويل بالنظر إلى مصدر الأمر بالتحويل إلى نوعين: الأول بالإضافة (Credit transfer)، والثاني بالخصم (Debit transfer). فالصورة الأولى تقوم على أساس قيام الآمر بالتحويل بتوجيه طلب للبنك (الذي يوجد له فيه حساب) بإضافة المبلغ المراد تحويله إلى حساب المستفيد، على أن تستقطع هذه القيمة من حساب الآمر بالتحويل، وهذه الصورة تستخدم بشكل واسع في المدفوعات التجارية، ودفع الرواتب لمستحقيها، وتوزيع أرباح الشركات (dividends company)، والصورة الثانية تقوم على أساس وجود تفويض من العميل للبنك، يقوم بموجبه البنك بإجراء التحويل بالخصم من حساب العميل بناء على طلب المستفيد بعد أن يقدم للبنك ما يفيد مديونية العميل له[٢].

---

(١) رأسم سميح محمد عبد الرحيم، مرجع سابق، ص١٠٦.

(2) **Ross Cranston**; Op. Cit, p. 235; **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 33. **William Gram**,; Op. Cit, p25.

٢١٩- وتجدر الإشارة إلى أن التحويل المصرفي للنقود قد شهد أطوارًا عدة في حياة البنوك. بل يمكن القول أن هذا النظام كان شاهدا على حركة التطور في نظام عمل البنوك في تفاعلها مع المعطيات المختلفة للتقدم في وسائل الاتصال، والتي سعت جاهدة إلى توظيف هذا التقدم في تنفيذ عمليات التحويل(١)، الأمر الذي يدعونا لتتبع خطى التطور الذي شهده هذا النظام، وذلك من خلال المرور سريعا على أشهر نظم التحويلات المصرفية للنقود، من أجل رسم صورة واضحة للتحويل الإلكتروني كإحدى العمليات المصرفية التي يقدمها البنك العامل عبر شبكة الإنترنت، باعتبارها امتدادًا لهذا التطور، وذلك على النحو التالي:

- نظام الحوالات السلكية (Wire Transfer):

يعد هذا النظام الخطوة الأولى على طريق التفاعل بين نظام نقل الأموال ووسائل الاتصال، حيث كانت عملية التحويل وتسوية المدفوعات فيما بين البنوك تتم وفقا لهذا النظام بصورة ورقية من خلال النقل بالبريد أو التلغراف(٢)، وقد بدأ العمل بهذا النظام في الولايات المتحدة الأمريكية في عام ١٩١٨، وذلك عندما بدأ بنك الاحتياطي الفيدرالي باستخدام التلغراف لإرسال واستلام التعليمات الخاصة بتحويل الأموال بين اثنتا عشر بنكا فيدراليا وقسم الخزانة (Department of treasury) التابع له. وقد تم إنشاء شبكة اتصالات تلغرافية آمنة لهذا الغرض(٣).

(1) **Thierry Moreau,** The emergence of a legal framework for electronic transactions, Computers & Security, 18 (1999) 423-428, p 424.

(2) **Adrian Mc Cullagh and William Caelli**; Op, Cit, p. 339.

(٣) وقد اعتمد هذا النظام على شفرة خاصة قام باختراعها العالم Samuel Morse، حيث كانت هذه الشفرة تتكون أحيانا من نقاط وعلامات مسلسلة، أو نغمات طويلة وقصيرة،

وأهم ما يميز هذا النظام هو السرعة والأمان في إجراء عملية التحويـل[1]. لكن الأمر في ضوء هذا النظام مقصور على إجراء عملية التحويـل، دون أيـة معلومات لشرح تفاصيل هذه العملية[2].

- نظام مقاصة المدفوعات بين البنوك:

The Clearing House Interbank Payments Systems (CHIPS):

وهذا النظام تعود ملكيته وإدارته لمجموعة من البنوك وبيـوت المقاصـة التابعـة لجمعيـة مقاصـة نيويـورك New York Clearing House Association، وهو نظام إلكتروني؛ حيث يعتمد في تشغيله على جهاز كمبيوتر مركزي متصل بنهايات طرفية في صورة شبكة داخلية تضم البنوك والمؤسسات المنضمة له. ويستخدم هذا النظام أساسا لإجراء الحوالات كبيرة الحجم، وعلـى وجه التحديد يستخدم في تسوية صفقات شراء وبيع النقود الاتحادية فيمـا بـين البنوك، وتسوية صفقات تبادل النقد الأجنبي، وأيضا في تسوية صـفقات تبـادل السندات المالية (securities transaction)[3]. لكن يعاب على هـذا النظـام

أو إشارات ضوئية، حيث جرى العمل على التنويع في أسلوب تركيب الشفرة من أجل الوصول إلى أعلى درجات الأمان في عمليات التحويل. انظر في تفصيل ذلك:

Charles A. Oswald; Op, Cit, p. 45.

(1) **Benjamin Geva**, The law of electronic funds transfers; Op. Cit, p. 2-6, 1-37

(٢) رأسم سميح محمد عبد الرحيم، التجارة الإلكترونية في خدمة التجـارة والمـصارف العربية، المرجع السابق، ص١٠١.

(3) **Charles A. Oswald**; Op, Cit, p. 46; **Tanai Khiaonarong**, Electronic payment systems development in Thailand, International

كسابقه إجراء عملية التحويل ببيانات بسيطة، دون أن تتضمن عمليـة التحويـل ذكر أية تفصيلات تخص بيانات وتعليمات عملية التحويل.

- نظام جمعية الاتصالات المالية العالمية لما بين البنوك:

Society for Worldwide Interbank Financial Telecommunications (SWIFT):

ونظام جمعية سويفت (Swift) كأحد الأنظمة المستخدمة في عمليات تحويل الأموال فيما بين البنوك يعتمد على شبكة اتصالات تربط البنوك المشتركة فيـه بخطوط اتصال دولية أمنة[١]. ويستخدم هذا النظام أساسا في المدفوعات الدولية، وتستخدم المصارف هذا النظام عادة في تسوية عمليات الدفع، من خلال إرسـال التعليمات والإشعارات الخاصة بهذه العمليات بشكل قياسي وموحـد ومتعـارف عليه بين البنوك الأعضاء في جمعية (SWIFT)[٢].

- نظام بيت المقاصة Automated Clearing House (ACH):

وبيت المقاصة عبارة عن شبكة إلكترونية لتحويل الأموال، تقوم على إدارة عدد كبير من المدفوعات من خلال التسوية بين الجانب الدائن والمدين لأطراف

Journal of Information Management 20 (2000), 66.

(1) **Francois Dentz**, la banque et l utilisation de Swift, transplis, No spécial, avril 1975, p. 43.

(٢) رأسم سميح محمد عبد الرحيم، مرجع سابق، ص ١٠٢؛

Jacques vanrenterghem, Un projet international de commutations de messages interbancaires, organization et technique bancaires, N 328-avril 1974, p 408.

التعامل. ويحكم نظام عمل هذه الشبكة القواعد والتعليمات الصادرة عن مؤسسة (NACHA)[1]. وتختص هذه الشبكة بإجراء عمليات التحويل المالي الدورية صغيرة الحجم؛ فهي تختص على وجه التحديد بدفع المرتبات من خلال القيد المباشر على حساب أصحابها، دفع أقساط التأمين، دفع الفواتير الخاصة ببعض العمليات، دفع الشيكات الإلكترونية[2]، وعلى الرغم مما يتميز به هذا النظام من مزايا إلا أنه يعاب عليه استغراقه لوقت طويل في إتمام عمليات التحويل، حيث تصل هذه المدة إلى يوم أو يومين[3].

ويتضح من خلال استعراض النظم السابقة أنها تدور في فلك ما يسمى التحويل الإلكتروني للأموال، الذي يقوم على أساس نقل مبلغ معين من حساب مصرفي إلى حساب آخر عن طريق شبكات إلكترونية داخلية يستفيد منها

---

(١) وهي جمعية أنشئت عام ١٩٧٤ لتقوم على تنسيق عمل شبكة دار المقاصة الآلية وتقدم الخدمات التعليمية لعملائها والمشاركين فيها، ويحكم عمل هذه الجمعية عقد إنشائها وقانون الصفقات الإلكترونية والقانون التجاري الموحد. انظر:

ACH transactions involving the internet, Guidance and examination procedures, Op. Cit, p. 6. available at: www.occ.treas.gov/ftp/bulletin/2004-58.txt ;**Request for public comment on a proposal to revise the official staff commentary to regultion- E (Electronic Fund Transfers),** Federal reserve bank of Dallas, Vol. 65, No. 126. July 20, 2000, p. 40062

(2) **Automated Clearing House**, wikipedia, free enclopedia, 2007, p 1. available at:

http://en.wikipedia.org/wiki/Automated_Clearing_House

Choi Stahl, Electronic payment systems, Whinston, 2003, p 2.

(٣) **رأسم سميح محمد عبد الرحيم**، مرجع سابق، ص١٠٣.

الأعضاء المنضمين لها فقط تحت إشراف بيوت وجمعيات المقاصة[١].

٢٢٠- ونلاحظ على النظم السابقة للتحويل المصرفي عدة ملاحظات على النحو التالي[٢]:

١- أن كل نظام من هذه النظم منغلق على من فيه[٣]. فالاستفادة من أي نظام مقصور فقط على الأعضاء المنضمين لهذا النظام دون غيرهم من البنوك غير المشتركة فيه. ويعود ذلك لطبيعة شبكة الاتصال التي تربط هؤلاء الأعضاء، حيث إنها شبكة داخلية تتكون من خطوط اتصال تربط بين الأعضاء وتعتمد على برامج تعمل بلغة لا يفهمها إلا هؤلاء الأعضاء فقط، ومن ثم إذا كان هناك أحد البنوك التي قد ترغب في إجراء عملية تحويل مع أحد البنوك الأعضاء (خاصة على صعيد معاملات التجارة الدولية) فلا تتمكن من الاستفادة من هذا النظام، الأمر الذي يمكن معه القول بافتقاد نظام موحد يتعامل بلغة واحدة في مجال التحويل الإلكتروني للأموال بين جميع البنوك.

٢- أن المقصود بالتحويل الإلكتروني في نظام عمل هذه البنوك- قبل ظهور البنك الإلكتروني- هو الاتصال فيما بين البنوك إلكترونيا لتنفيذ عملية التحويل (أي نقل المبلغ من حساب لآخر)، على أن يظل اتصال العميل الآمر بالتحويل بالبنك، واتصال البنك بالمستفيد بصورة ورقية.

---

(1) **U.S. Consumers and electronic banking**, 2003, available at: www.federalreserve. gov/pubs/bulletin/2004/winter04_ca.pdf

(٢) **رأسم سميح محمد عبد الرحيم**، مرجع سابق، ص١٠٦؛

Francois Dentz; Op. Cit, p. 43.

(3) **G C Chalikias**; Op, Cit, p. 2.

٣- أن معظم النظم السابقة تقوم على فكرة إجراء التحويل دون أن يكون مرفقا به البيانات الخاصة بهذه العملية. على الرغم مما لهذه البيانات من أهمية تعادل أهمية عملية التحويل ذاتها، وتظهر هذه الأهمية من خلال قدرة العميل فيما بعد على مطابقة التحويل بالصفقات التي قام بعملية التحويل بمناسبتها.

٢٢١- وانطلاقا من الملاحظات السابقة على أنظمة التحويل الإلكتروني، يمكن القول بأن هذه الأنظمة لم تعد تتلائم مع أساليب تنفيذ المعاملات التجارية، التي شهدت تطورا كبيرا أنعكس بالتبعية على نظم الدفع بأشكالها المختلفة بوجه عام، وعلى التحويل الإلكتروني بوجه خاص، الأمر الذي جعل للتحويل الإلكتروني للنقود مفهوما جديدا، استطاعت البنوك الإلكترونية العاملة عبر شبكة الإنترنت أن تستوعبه، وذلك بفضل ما تتمتع به هذه البنوك من قدرة فائقة على التواصل وتبادل البيانات والمدفوعات فيما بينها من ناحية، وفيما بين عملائها من ناحية آخري. وهذا المفهوم في ظل عمل هذه البنوك يتجلى في عدة أمور على النحو التالي:

(١) تبنى نظام موحد للتحويل الإلكتروني للنقود فيما بين المتعاملين على الصعيد المحلي والدولي. وذلك على النحو الذي يجعل الاستفادة من نظام التحويل متاحة أمام كافة البنوك المتصلة بشبكة الإنترنت، ودون الحاجة إلى الانضمام إلى اتحادات أو جمعيات معينة، أو الاتفاق على صيغة خاصة تتم من خلالها عمليات التحويل، ولاشك في أهمية التحويل بهذا المعنى ليس لخدمة التجارة الإلكترونية فقط، ولكن لخدمة التجارة الدولية أيضا، حيث كانت الحاجة ماسة لكل منهما إلى نظام للتحويل يعرف لغة مشتركة في التعامل يعلمها الجميع

ويتقيدون بأساليب عملها. وقد تمكنت البنك الإلكتروني من أن تحقق ذلك بفضل اتساع شبكة الإنترنت التي تربط أطراف العالم المترامية من ناحية، وبفضل البرمجيات والبروتوكولات التي تقوم عليها هذه البنوك من ناحية أخرى[1].

(٢) أصبح مصطلح التحويل الإلكتروني في نظام عمل البنك العامل عبر شبكة الإنترنت يشتمل ليس فقط على اتصال البنوك إلكترونيا فيما بينها لنقل مبلغ التحويل من حساب مصرفي لآخر، ولكن أيضا تواصل الأطراف الأخرى(الآمر بالتحويل، والمستفيد) مع هذه البنوك إلكترونيا لإصدار واستلام بيانات وتعليمات التحويل[2]، الأمر الذي أضفى على التحويل مفهوم الدفع الإلكتروني[3]، حيث بفضل هذا التواصل الإلكتروني يستطيع العميل بعد إجراء الصفقات الإلكترونية أن يقوم بدفع المبلغ المستحق في ذمته بتحرير شيك إلكتروني بالمبلغ المستحق، أو الدفع من خلال بطاقة الائتمان، أو من خلال الاتصال إلكترونيا عن طريق برامج التحويل الخاصة المثبتة على الجهاز الخاص بالعميل، والمتصلة بالبنك عن طريق شبكة الإنترنت[4]. وقد

---

(1) **Michael Chissick, Alistair Kelman**; Op. Cit, p. xxxviii.

انظر أيضا العنوان الإلكتروني التالي:

http://www.al-jazirah.com/digimag/15062003/agtes17.htm

(2) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 32.

(3) **Meiring, Gezina Aletta,** Legal aspects of the computerisation of the payment system, Dissertation presented to University of South Africa (South Africa), DAI-A 61/03, Sep 2000, p10; **Dan Zhu**, Security control in inter-bank fund transfer, Journal of electronic commerce research, vol. 3, No.1, 2002, p 15.

(4) **FCIC: Electronic Banking,** Electronic fund transfers, p 1avaliable

أدى هذا إلى تقديم العديد من المنافع والتي تمثلت في إيجاد نوع من تنظيم عمليات الدفع (on-time payments)، حيث يمكن للبنك الإلكتروني أن يقوم باقتطاع وتسديد قيمة التحويلات النقدية إلكترونيا بصورة منتظمة وفي الأوقات المحددة لذلك على نحو أكثر فعالية بالمقارنة بعمل البنوك التقليدية. علاوة على ذلك توفير السلامة والأمن (safety & security)، حيث تتم عملية التحويل الإلكتروني للنقود من قبل البنك الإلكتروني عن طريق شبكة الإنترنت وفق نظم أمنية تكفل سرية وأمن المعلومات والبيانات الخاصة بعملية التحويل. يضاف إلى ذلك قلة التكاليف التي يتحملها العميل نظير الحصول على خدمة التحويل الإلكتروني الذي يتم عبر شبكة الإنترنت من قبل البنك الإلكتروني(1).

(٣) التحويل الإلكتروني في نظام عمل بنوك الإنترنت لم يعد قاصرا على مجرد تبادل بيانات وأرقام محاسبية بين البنوك تفيد نقل مبلغ معين من حساب مصرفي لحساب آخر، بل أصبح- بفضل ما توفره شبكة الإنترنت من مزايا في التواصل بين المتعاملين من خلالها- يشتمل على كافة البيانات

at: http://www.pueblo. gsa.gov/cic_text/mony/e-banking/bank.htm; **Fram bureau bank FSB**, FBB internet banking access agreement and electronic fund transfer act disclosure, available at :www.farmbureaubank.com/docs/disclosures/IB_Agreement.pdf; **Request for public comment on a proposal to revise the official staff commentary to regulation- E (Electronic Fund Transfers)**;Op. Cit, p 40061

(١) انظر العنوان الإلكتروني التالي :
http://www.itep.ae/arabic/EducationalCenter/CommNet/eft.asp

والمعلومات الشارحة لتفصيلات عملية التحويل[١]، حيث كان نظام التحويل في ظل الشبكات الخاصة يكتفي بمجرد تبادل البيانات الخاصة بنقل المبلغ من حساب لآخر فقط- وذلك بحكم تصميم هذه الشبكات وبحكم البرامج المتحكمة في تشغيلها- الأمر الذي لا يتحقق في نظام عمل شبكة الإنترنت، التي يمكن من خلالها ليس فقط تبادل البيانات الخاصة بقيد المبلغ، ولكن أيضا كافة البيانات والمعلومات الشارحة لتفصيلات عملية التحويل. وكما سبق أن ذكرنا الأهمية الكبيرة لهذا الأمر والتي تتمثل في أن العديد من الشركات والمؤسسات لا تستطيع أن تطابق التحويل مع أي صفقة إلا إذا صاحب هذا التحويل البيانات والمعلومات الشارحة الخاصة بتسوية الصفقة المتعلقة بالتحويل[٢].

وفى ضوء ما سبق ذكره يتضح أن التحويل المصرفي للنقود بداية من النظام الورقي وانتهاءً بالنظام الإلكتروني عبر شبكة الإنترنت، يحتفظ بذات المضمون من كونه عملية تؤدى إلى نقل مبلغ من النقود بين حسابين لدى ذات البنك، أو بين بنكين مختلفين وأن وجه الاختلاف هي في الوسيلة المتبعة في تواصل أطراف عملية التحويل، بداية من إصدار أمر التحويل، وانتهاءً بتنفيذه[٣].

وبناءً عليه يمكن أن يعرف التحويل الإلكتروني للنقود في نظام عمل البنك العامل على شبكة الإنترنت بأنه عبارة عن نقل الدفعات النقدية من حساب بنكي إلى حساب بنكي آخر، إضافة إلى نقل المعلومات المتعلقة بهذا النقل، بناء على

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 33.

(٢) راسم سميح محمد عبد الرحيم، مرجع سابق، ص١٠٨

(3) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 32.

أمر الآمر بالتحويل لمصلحة المستفيد وذلك عبر شبكة الإنترنت(١).

ويتضح من خلال التعريف أن التحويل يتم في مواجهة أربعة أشخاص، العميل الآمر بالتحويل، والبنك الإلكتروني الذي يصدر إليه الأمر بالتحويل والذي يقوم بتنفيذه عن طريق إجراء القيد، والبنك المحول لديه، والمستفيد، أي المحول له، مع ملاحظة أنه في حالة ما إذا كان التحويل يتم بين حسابين داخل ذات البنك فإنه يتم بين ثلاثة أشخاص؛ الأمر بالتحويل والبنك والمستفيد(٢).

المطلب الثاني

كيفية إجراء عملية التحويل الإلكتروني للنقود في نظام عمل بنك الإنترنت

٢٢٢- تشهد عملية التحويل الإلكتروني للنقود كإحدى العمليات المصرفية التي يقوم بها البنك الإلكتروني على شبكة الإنترنت مرحلتين، الأولي: وهي مرحلة الأمر بالتحويل، والثانية: هي مرحلة القيد المزدوج على التفصيل التالي:

أولا- مرحلة الأمر بالتحويل:

٢٢٣- تتمتع مرحلة الأمر بالتحويل في نظام عمل البنك الإلكتروني العامل عبر شبكة الإنترنت بخصوصية معينة، ويتجلى ذلك بإصدار العميل هذا الأمر للبنك

---

(١) نظام التحويلات المالية الإلكترونية، مقالة متاحة على العنوان الإلكتروني التالي:
http://www.al-jazirah.com/digimag/15062003/agtes17.htm.

(2) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 32.

إلكترونيا عن طريق شبكة الإنترنت، الأمر الذي لم يكن معروفا من قبل حيث كانت المراسلات الورقية هي اللغة السائدة والحاكمة للتعامل فيما بين العميل والبنك بخصوص أمر التحويل. ولا شك فيما يشكله الاتصال الإلكتروني في هذه المرحلة من فوائد عدة سواء بالنسبة للعميل (الآمر بالتحويل) أم بالنسبة للبنك الإلكتروني، حيث يتميز هذا الاتصال بالسهولة والبساطة في التعامل، بالإضافة إلى قلة التكاليف الناشئة عن ذلك(١) ويعلو على كل هذه الفوائد الأمن والسلامة الناتجة عن توجيه هذا الأمر للبنك عبر شبكة الإنترنت، مما يجنب العميل مخاطر كانت تتعرض لها الأوراق والمستندات التي تثبت عملية التحويل كالسرقة أو الضياع.

أما بالنسبة لأوجه استفادة البنك الإلكتروني من ذلك فهي عديدة، كقلة التكاليف والسهولة في التعامل، لكن الأهم من كل هذا، هو تعدد الوسائل التي يمكن من خلالها للعميل طلب خدمة التحويل من البنك، بل يمكن القول بأن العديد من صور الدفع الإلكتروني الموجهة للبنك عبر شبكة الإنترنت ما هي في حقيقة الأمر إلا توجيه أمر بالتحويل من العميل للبنك بخصوص مبلغ الدفع(٢).

٢٢٤- وتتعدد الصور التي من خلالها يستطيع عملاء البنك الإلكتروني إرسال أوامر التحويل لأموالهم للبنك الإلكتروني عبر شبكة الإنترنت، وذلك على النحو التالي(٣):

---

(1) **Ross Cranston**; Op, Cit, p. 287.

(2) **Meiring, Gezina Aletta;** Op, Cit, p. 10; **FCIC: Electronic Banking,** Electronic fund transfers, p 1avaliable at: http://www.pueblo.gsa.gov/cic_text/mony/e-banking/bank.htm

(3) **Donald l. Baker, Roland E. Brandel,** The law of electronic fund

١- يستطيع عملاء البنك الإلكتروني إجراء التحويل الإلكتروني لأموالهم باستخدام بطاقات السحب النقدي ATM Cards، وذلك من خلال مكائن السحب الآلي (Automated teller Machines) المتواجدة في أماكن مختلفة، والمتصلة بالبنك عن طريق شبكة الإنترنت، والتي تعمل على مدار اليوم(١).

ولبطاقة السحب النقدي العديد من الوظائف(٢)، من أهمها التحويل

---

transfer systems, Alex e Solutions. inc, 2008, p. 1; **Charles A. Oswald**; Op, Cit, p. 53; **Adrian McCullagh -William Caelli**; Op. Cit, p. 337; **Request for public comment on a proposal to revise the official Staff commentary to regulation- E (Electronic Fund Transfers)**; Op. Cit, p. 40061

(1) **FCIC: Electronic Banking,** Electronic fund transfers, p1. available at: http://www. pueblo.gsa.gov/cic_text/mony/e-banking/bank.htm; **Ronald J. Mann**, Regulating internet payment intermediaries, (ICEC) Pittsburgh, PA, 2003, p 378.

- وعن الآلية التي تعمل بها مكائن سحب النقود في نظام عمل البنك العامل عبر شبكة الانترنت فإنها تعمل بنظام واجهة الاتصال عن بعد ("Remote interface)، حيث تظهر الماكينة في صورة صندوق يحتوى على جهاز صراف آلي متواجد في أماكن معينة (كالمطارات، وأماكن التسوق) ومؤمن بصورة جيدة، ومتصل بالبنك لاسلكيا بشبكة الانترنت، لإجراء المعاملات المصرفية من خلال هذه الماكينة، وقد أقرت الدائرة الاتحادية لمحكمة الاستئناف الأمريكية هذا التوصيف لهذه المكائن.

United States Court of Appeals for the Federal Circuit, Decisionning.com, inc., 2007-1277, p 11

(٢) ومن أهم هذه الوظائف، استخدامها في سحب النقود من أي مكان، استخدامها في إيداع النقود، معرفة معلومات عن حالة الرصيد، سداد الفواتير المستحقة، وغيرها من الخدمات التي يمكن للبنك تقديمها للعميل عن بعد. انظر مزيد من التفصيل:

Lucas D. Introna & Louise Whittaker, Power, Cash, and Convenience: Translations in the Political Site of the ATM, Taylor & Francis Group, LLC, 2006,p 338

الإلكتروني للنقود. ويمكن توجيه أوامر هذا التحويل باستخدام هذه البطاقة على النحو التالي:

أ- حيث يمكن لحامل هذه البطاقة (Card holder) أن يقوم بشراء ما يحتاج إليه من سلع وخدمات ثم يدفع ثمنها من خلال تحويل المبلغ المستحق للتاجر إلى الحساب المصرفي الخاص به من خلال الخصم الفوري من الحساب المصرفي الخاص بحامل البطاقة، حيث تتم هذه العملية من خلال قيامه بإدخال بطاقة (ATM) في جهاز السحب الآلي الخاص بالبنك الإلكتروني والموجود لدى التاجر، ثم بإدخال الرقم السري الخاص باستعمال البطاقة[1]، فيقوم جهاز السحب الآلي المتصل بقاعدة البيانات الخاصة بالبنك الإلكتروني عبر شبكة الإنترنت، بخصم المبلغ المستحق من حساب حامل البطاقة وإضافته في حساب التاجر[2].

ب- كما يمكن لحامل البطاقة الصادرة عن البنك الإلكتروني استعمالها في جهاز إخبار آلي(Automated teller Machines) مملوك لبنك آخر (The acquirer) (وذلك بموجب اتفاق بين البنكين يسمح بذلك)، وذلك لسحب مبلغ معين من هذا البنك، حيث يقوم الأخير- بعد التأكد من صحة البطاقة، والحصول على بياناتها- بتسوية هذه العملية مع البنك الإلكتروني المصدر

(1) **Consumer rights in electronic fund transfers**, California department of consumer affairs division of legal affairs(Legal Guide CR-6): Op. Cit, p. 1.

(2) **Meiring, Gezina Aletta** ; Op, Cit, p. 35.

لهذه البطاقة عن طريق التحويل الإلكتروني(١).

والغالب ما يكون العميل مقيدا من قبل البنك باستعمال البطاقة في حدود مبلغ معين، لكن هذا لا يمنع من قيام البنك بمنحه ائتمانا في حدود معينة، سواء كان لديه رصيد يغطي هذا أم لا(٢).

٢- يمكن لعميل البنك أيضا أن يوجه للبنك أمر التحويل عن طريق جهاز الكمبيوتر الخاص به، والمتصل بشبكة الإنترنت وذلك عن طريق:

أ- برنامج الدفع الإلكتروني المثبت على جهاز العميل، وهو برنامج خاص يسمح للعميل بإصدار أوامر التحويل للبنك عبر شبكة الإنترنت، حيث يجرى نظام العمل بهذا البرنامج على أن يقوم العميل بعد إرسال طلب لشراء بضائع معينة للتاجر (والذي يشتمل على البيانات الخاصة بهذا العميل والتي من أهمها البنك الإلكتروني الذي يتعامل معه)، يقوم التاجر بإرسال إيصال دفع إلكتروني إلى بنك العميل، على أن يقوم الأخير بعد التحقق من هذا الإيصال، بإرسال إيصال وفاء إلى العميل ليقوم بقبول هذا الإيصال وإعادة إرساله للبنك عن طريق برنامج الدفع(٣).

---

(١) د. **منظور أحمد حاجي الأزهري**، بطاقة السحب النقدي، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ ١٠-١٢ مايو ٢٠٠٣ دبي، ص ٣٦٩.

(2) **Meiring, Gezina Aletta;** Op, Cit,p. 35.

(٣) ومن أشهر هذه البرامج برنامج (Klebx)، وهذا البرنامج تم اقتراحه من قبل شركة مصرفية تسمى (Kleline) وذلك من أجل استخدامه في عمليات تسوية الديون التجارية. انظر مزيدا من التفصيل. د. **عدنان إبراهيم سرحان**،الوفاء (الدفع) الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي،

ب-يستطيع العميل أيضا أن يوجه أوامر التحويل للبنك عن طريق جهاز الكمبيوتر الخاص به، وذلك من خلال إرسال رسالة إلكترونية عبر البريد الإلكتروني تفيد ذلك[١]، فإذا كان العميل هو المدين فإنه يطلب من البنك بتحويل الدفعة من حسابه إلى حساب المستفيد، سواء كان الأخير لديه حساب لدى ذات البنك، أم كان لدى بنك آخر، أما إذا كان هو الدائن فإنه يطلب من البنك تحصيل المبلغ المستحق من بنك المدين، مع قيام العميل بإرسال كافة المستندات التي تثبت استحقاقه لهذا المبلغ[٢].

٣- ويستطيع العميل كذلك إصدار أوامر التحويل للبنك باستخدام بطاقة الوفاء في أماكن البيع point of sale (POS) [٣]، وتتم هذه العملية عند شراء العميل ما يحتاج إليه من سلع أو خدمات من أحد المتاجر(سواء من المتاجر التقليدية أم الافتراضية)، ثم يستعمل بطاقة الوفاء(Debit Card) الصادرة له من البنك الإلكتروني، لدفع المبلغ المستحق عليه، وذلك من خلال التوقيع على قسيمة أو فاتورة الشراء التي يعدها له التاجر، بعد أن يتأكد من صحة البطاقة ومن شخصية حاملها، حيث يقوم التاجر بعد ذلك بإرسال طلب تسوية مرفقا به القسيمة أو الفاتورة إلى البنك الإلكتروني، ليتم خصم القيمة

ص٢٧٢.

(1) **Benjamin Geva**, The law of electronic funds transfers; Op, Cit ,P1-28

(٢) **د. بلال عبد المطلب**، مرجع سابق، ص ١٩٦٤

(3) **Benjamin Geva**, The law of electronic funds transfers; Op, Cit ,P1-27; **FCIC: Electronic Banking,** Electronic Fund Transfers, p 1avaliable at: http://www.pueblo.gsa.gov/cic_text/ mony/e-banking/bank.htm

المستحقة من حساب العميل وإضافتها في حساب التاجر[1].

٤- يمكن للعميل علاوة على ذلك إصدار أمر التحويل إلى البنك عن طريق تحرير شيك إلكتروني. حيث يسلم البنك الإلكتروني العميل بموجب ما لديه من رصيد لدى البنك دفتر شيكات إلكتروني، حيث يستطيع العميل التعامل على الحساب الخاص به والموجود لدى البنك بموجب هذه الشيكات. وتتم هذه العملية من خلال ملء العميل فراغات نموذج الشيك الإلكتروني وإرساله للمستفيد (المحول له)، حيث يقوم الأخير بإرسال الشيك للبنك الصادر عنه (حيث يحمل الشيك البيانات الخاصة بهذا البنك)، والذي يقوم بموجب هذا الشيك بقيد المبلغ الثابت فيه في الجانب المدين من حساب مصدر الشيك، وفي الجانب الدائن من حساب المستفيد، وذلك إذا كان لكل منهما حسابين لدى ذات البنك. أما إذا كان للتاجر حساب لدى بنك آخر، فيجب على البنك أن يضع المبلغ تحت تصرف بنك المستفيد في الجانب الدائن[2].

ويلاحظ أن العميل يمكن أن يطلب من البنك الإلكتروني إجراء عملية تحويل فردية (transfer single)، وهي عملية تحويل تتم مرة واحدة لفرد محدد

(١) **د. محمد عبد الحليم عمر**، بطاقات الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص٦٦٦.

(2) **FCIC: Electronic banking**; Op. Cit., p. 2; **Request for public comment on a proposal to revise the official staff commentary to regulation-E (Electronic Fund Transfers)**: Op. Cit, p. 40062; **Benjamin Geva,** Recent international developments in the law of negotiable instruments and payment and settlement systems; Op. Cit, p. 687.

أو يطلب إجراء عملية تحويل منتظمة (Regular transfers) وهي عملية تحويل تتم على فترات منتظمة (كرواتب أو أقساط لمبالغ معينة)[1].

٢٢٥- وأيا ما كان الطريق الذي يسلكه العميل لتوجيه الأمر بالتحويل، فإن هذا الأمر يجب أن يشتمل على البيانات الخاصة بهذا العميل، والتي تساعد البنك في التعرف على شخصيته (كاسمه، ورقم حسابه، توقيعه الإلكتروني)[2]، أيضا يجب أن يشتمل الأمر على المبلغ المراد نقله واسم المستفيد ورقم حسابه، بالإضافة إلى مكان وتاريخ إصدار هذا الأمر[3].

ثانيًا- مرحلة القيد (Settlement):

٢٢٦- تعرف مرحلة القيد أو التسوية بأنها قيد المبلغ المراد نقله في جانب خصوم العميل الآمر بالنقل وفي جانب الأصول من حساب المنقول إليه[4]، وترتبط مرحلة القيد بهذا المعنى ارتباطا لا يقبل التجزئة بمرحلة الأمر بالتحويل في نظام التحويل الإلكتروني للنقود، بحيث يمكن القول إن أمر العميل بالتحويل لا يرتب أي حق للمحول له إلا بإجراء القيد أو التسوية[5].

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 33.

(2) **Fram Bureau Bank FSB**, FBB internet banking access agreement and electronic fund transfer act disclosure, Op. Cit.

(3) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 35.

(٤) **د. عبد الفضيل محمد أحمد**،الأوراق التجارية وعمليات البنوك، دار النهضة العربية، ص٤٦٧.

(٥) ومن هذه الزاوية يظهر الاختلاف بين الدفع من خلال الشيك كورقة تجارية، وبين تحويل النقود، حيث إن تحرير الشيك يجعل للمستفيد حقا على مقابل الوفاء (الرصيد) بمجرد تمام عملية التحرير، بحيث يمكن القول إن الحق المصرفي ينتقل من الساحب إلى المستفيد بمجرد تحرير الشيك، أما في تحويل الأموال فإن المستفيد لا يتقرر حقه

والتسوية قد تتم داخل البنك الإلكتروني ذاته، وذلك في حالة ما إذا كان للآمر بالتحويل حسابان، وطلب إجراء التحويل من أحد الحسابين للآخر، أو يكون الأمر بالتحويل والمحول له لديهم حسابات لدى ذات البنك الإلكتروني، حيث سيقوم الأخير فقط بقيد المبلغ المحول في جانب الدائن من حساب المستفيد، وقيد ذات المبلغ في جانب المدين من حساب العميل الآمر، أي بنقل قيمة التحويل من حساب الأمر بالتحويل لحساب المحول له[1].

٢٢٧- أما إذا كان لكل من الآمر بالتحويل والمستفيد لهما حسابات لدى بنوك مختلفة فإن التسوية تتم فيما بين البنوك على النحو التالي:-

إما أن تتم التسوية بصورة ثنائية (Bilateral settlement) وذلك إذا كان بين بنك الآمر بالتحويل وبنك المستفيد حسابات مشتركة، أي كان لأحد البنكين حساب لدى الأخر، حيث ستتم عملية التسوية فيما بين البنكين إلكترونيا عن طريق شبكة الإنترنت، وذلك من خلال قيام بنك الأمر بالتحويل بإرسال كافة المستندات التي تفيد حق بنك المستفيد في الحصول على الدفعة محل عملية التحويل، وتتم عملية التسوية بين البنكين في هذه الحالة في ضوء الاتفاقات التي تحكم عملية التحويل الإلكتروني للأموال عبر شبكة الإنترنت بينهما (مع ملاحظة أن هذه الاتفاقات والتعاقدات تتم بين البنوك بصورة إلكترونية) [2].

وإما أن تتم التسوية بصورة متعددة الأطراف (Multilateral

على المبلغ المحول بمجرد صدور الأمر بالتحويل، بل يلزم لذلك إجراء القيد المزدوج في الحسابين.

(١) **د. بلال عبد المطلب**، المرجع السابق، ص ١٩٦٥.

(2) **Benjamin Geva**, The law of electronic funds transfers, Op. Cit, p. 1-28

settlement)، وهي التسوية التي تتم من خلال القيد في دفاتر المراسلات المشتركة، والتي عادة ما تتواجد لدى البنك المركزي الذي يحتفظ بحسابات مشتركة للبنوك الأطراف في عملية التحويل. وإذا كانت التسوية الثنائية تتم فيما بين البنوك عبر تبادل الرسائل الإلكترونية بصورة مباشرة، فإن التسوية المتعددة الأطراف تتم بتوجيه المراسلات الإلكترونية للبنك المركزي عن طريق شبكة الإنترنت، أي أن التعامل لا يتم بصورة مباشرة بين بنك الآمر بالتحويل وبنك المحول المستفيد(١).

أما إذا كان الأمر يتعلق بعلاقة دولية فإن عملية التسوية فيما بين البنوك تتم عن طريق الهيئات الدولية، حيث عن طريق هذه الهيئات تتم عملية المقاصة والتسويات الإلكترونية وتحويل النقود بين بنك الآمر بالتحويل وبنك التاجر، ومن أكثر هذه الهيئات انتشارا " فيزا" "ماستر كارد"(٢).

وبعد أن تتم عملية التسوية فيما بين البنوك عبر شبكة الإنترنت، يلتزم كل من بنك الآمر بالتحويل وبنك المستفيد بأن يخطر كل منهما عميله بحالة حسابه وما طرأ عليه من زيادة أو نقص مدعومة بالإيصالات والمستندات المؤرخة التي تثبت إجراء عملية التحويل(٣).

---

(1) **Ross Cranston,** Principles of banking law, Op. Cit,. p. 287.

(٢) **ثناء أحمد محمد المغربي**، الوجهة القانونية لبطاقات الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠-١٢ مايو ٢٠٠٣م، غرفة تجارة وصناعة دبي، ص ٩٤٦.

(3) **FCIC: Electronic Banking,** Electronic Fund Transfers, Op, Cit, p. 3; **Hanmi internet bank,** Hanmi internet banking service agreement, cancellation-termination of service, p. 5, available at:_

وبعد الانتهاء من بيان عملية التحويل الإلكتروني بمرحلتيها، يطفو على سطح البحث تساؤل يعالج حالة فسخ العميل للصفقة التجارية التي كانت سببا في قيامه بالتحويل الإلكتروني لقيمة الصفقة في حساب من يتعامل معه. هل يحق للعميل أن يطلب من البنك إلغاء عملية التحويل؟

٢٢٨- قبل الإجابة على هذا التساؤل نود أن نشير إلى أن الأصل والقاعدة هي أن البنك بمجرد تلقيه أمر التحويل يجب عليه أن يبادر إلى تنفيذه (بالقيد والخصم)، مادام هناك رصيد كاف يسمح بذلك؛ لكن هذا لا يمنع من إمكانية اتفاق البنك وعميله على إرجاء تنفيذ أوامر التحويل الصادرة من الآمر أو المقدمة من المستفيد إلى آخر اليوم لتنفيذها مع غيرها من الأوامر التي من نوعها والصادرة في ذات اليوم[1]، ومن ثم من المتصور وجود فاصل زمني بين تلقي أمر التحويل وتنفيذه.

وبخصوص الإجابة على التساؤل السابق، فالملاحظ على العقود التي تحكم علاقة البنك الإلكتروني بعميله بخصوص خدمة التحويل الإلكتروني للنقود، أن هذه البنوك استغلت الفاصل الزمني الذي يوجد بين إصدار الأمر وتنفيذه بأن أعطت العميل الحق في إلغاء أمر التحويل. وقد وضعت هذه البنوك الخطوات التي يجب على العميل القيام بها لتحقيق ذلك (والتي تشتمل على بيان الوقت المناسب، والطريقة التي يخاطب بها البنك لإلغاء عملية التحويل، سواء من خلال البريد الإلكتروني أم الاتصال التليفوني، والمدة القانونية المسموح تقديم الطلب

---

http://www.hanmi.com/files/hanmibankinternetbankingapplication.pdf

(١) انظر نص المادة ٣٣٤، ٣٣٥ من قانون التجارة المصري رقم ١٧ لسنة ١٩٩٩.

خلالها)، والتي يقوم البنك بتوضيحها للعميل على الموقع الإلكتروني الخاص به على شبكة الإنترنت[1]. لكن الملاحظ أكثر على هذه العقود أنها ربطت إمكانية إيقاف أو إلغاء عملية التحويل بوصول طلب العميل للبنك قبل قيام الأخير بخصم قيمة التحويل من حسابه[2]، أي قبل تنفيذ أمر التحويل.

وحسنا فعلت هذه البنوك بأن اشترطت وصول طلب الإلغاء قبل إجراء الخصم من حساب العميل، حيث يتسق ذلك مع طبيعة عملية التحويل؛ والتي سبق أن ذكرنا أنها لا تتم بمجرد قيام الآمر بالتحويل بتوجيه الأمر للبنك، ولكن بعد تمام عملية القيد في حساب المستفيد.

وبناءً عليه، يجب على البنك الإلكتروني أن ينظم هذا الحق للعميل لمواجهة مختلف الظروف التي قد يضطر معها لإلغاء أو إيقاف عملية التحويل، وذلك على النحو الذي يمكن العميل من الاستفادة من هذا الحق في ضوء طبيعة نظام التحويل، وفي ضوء طبيعة الوسيلة الإلكترونية (شبكة الإنترنت) المستخدمة في تنفيذه. بأنْ يعطى للعميل الحق في إلغاء التحويل مادامت عملية القيد لم تتم بعد، بحيث تنعقد مسئولية البنك عن المبالغ المحولة بعد وصول إخطار العميل له وقبل القيام بالقيد. أما إذا كانت عملية القيد قد تمت بالفعل، فلا يحق للآمر بالتحويل الرجوع على البنك في هذه الحالة، وليس أمامه سوى الرجوع على المستفيد بدعوى دفع غير المستحق أو الإثراء بلا سبب، لانعدام السبب القانوني الذي

---

(1) **FCIC: Electronic Banking,** Electronic fund transfers ,Op. Cit p 2
- د. **محمد سعدو الجرف**، أثر استخدام النقود الإلكترونية على الطلب على السلع والخدمات، مرجع سابق، ص٢٠٠

(2) **Fram Bureau Bank FSB,** FBB internet banking access agreement and electronic fund transfer act disclosure, available at: www.farmbureaubank.com/docs/disclosures/IB_Agreement.pdf

يبرر حصول المستفيد على المبلغ، بعد فسخ العلاقة بينهم.

ونظرا لأهمية الطلب المقدم من العميل للبنك بإلغاء أو إيقاف عملية التحويل، فإن البنك يطلب من العميل ضرورة إفراغ طلبه هذا في نموذج مكتوب وموقع عليه من قبل العميل بما يفيد انصراف إرادته صراحة تجاه هذا الطلب. لكن هذا لا يمنع من سماح البنك للعميل بأن يخطره برغبته هذه بوسيلة سريعة كالبريد الإلكتروني أو الاتصال التليفوني، على أن يقوم العميل بعد ذلك بكتابة الطلب للبنك على النحو المطلوب[1]، مع ملاحظة أن أثر الإخطار يبدأ من لحظة إبلاغ العميل البنك بالإلغاء أو الإيقاف، وليس من وقت وصول الطلب المكتوب للبنك.

المطلب الثالث

التزامات أطراف عملية التحويل الإلكتروني

٢٢٩- بعد أن عرضنا لماهية التحويل الإلكتروني للنقود كإحدى العمليات المصرفية التي يقدمها البنك الإلكتروني العامل على شبكة الإنترنت، من خلال تعريف هذه العملية، وبيان للمراحل التي تمر بها بداية من إصدار العميل أمر التحويل الإلكتروني للبنك، وانتهاءً بقيد عملية التحويل بما يفيد نقل المبلغ المحول

---

(1) (If you make your stop-payment request online or by telephone, we may also require you to put your request in the form of paper writing and get it to us within 14 days after you call). **Fram Bureau Bank FSB**, FBB internet banking access agreement and electronic fund transfer act disclosure, available at: www.**farmbureaubank**.com/docs/ disclosures/IB_Agreement.pdf.

من حساب الأمر بالتحويل لحساب المستفيد، يثور التساؤل حول طبيعة التزامات ومسؤوليات أطراف هذه العملية؟

لكن الإجابة عن هذا التساؤل تفرض علينا أن نحدد الطبيعة القانونية لعلاقات أطراف عملية التحويل الإلكتروني، وذلك لأن تحديد طبيعة هذه العلاقات من شأنه أن يصل بنا لرؤية واضحة ومحددة لالتزامات ومسؤوليات أطراف هذه العملية.

وتجدر الإشارة إلى أن النظام القانوني المصري يخلو من نص ينظم التحويل الإلكتروني للنقود كإحدى العمليات المصرفية التي يقدمها البنك العامل عبر شبكة الإنترنت، الأمر الذي يدعو في سبيل وضع تنظيم قانوني لهذه العملية، إلى النظر في مدى استيعاب القواعد العامة في القانون المصري لتنظيم هذه العملية، والوضع في النظم القانونية الأخرى التي نظمت هذا الموضوع، أو ما استقرت عليه عقود التحويل الإلكتروني المصرفية.

١- طبيعة العلاقة القانونية بين الأمر بالتحويل والبنك الإلكتروني:

٢٣٠- قبل أن نسترسل في عرض الاتجاهات التي تتنازع تحديد طبيعة العلاقة بين الآمر بالتحويل والبنك الإلكتروني، نلاحظ بعد التعرف على مفهوم ومراحل التحويل المصرفي الإلكتروني كإحدى العمليات المصرفية التي يقدمها البنك العامل عبر شبكة الإنترنت، أن هذه العملية لم تشهد تغيرا في مضمونها عما كان عليه الحال في نظام عمل البنوك التقليدية (نقل مبلغ معين من حساب مصرفي إلى حساب آخر)، لكن التغيير كان في الطريقة أو الكيفية التي تسير بها هذه العملية سواء بين البنك والعميل أو بين البنوك بعضها البعض. مما انعكس على شكل الالتزامات الواقعة على أطراف العملية بحكم طبيعة الوسيلة المستخدمة في

تنفيذها، مع احتفاظ هذه العملية بمضمونها.

ويذهب البعض في تكييف علاقة العميل (الآمر بالتحويل) بالبنك الإلكتروني بأنها تعد من قبيل حوالة الحق، العميل فيها هو المحيل، والمستفيد من التحويل هو المحال له، والبنك القائم بعملية التحويل هو المحال عليه. وقد قيل ردا على هذا الرأي أنه يعطى للبنك باعتباره محالاً عليه الحق في أن يتمسك في مواجهة المستفيد باعتباره المحال له بكل الدفوع التي كان له أن يدفع بها في مواجهة الأمر بالتحويل وهو المحيل. وكان هذا النقد كافيا لاستبعاد نظرية حوالة الحق(1) ونضيف على ما وجه لهذه النظرية من نقد الطبيعة الخاصة التي تحكم علاقة البنك الإلكتروني بعميله، والتي على أثرها قد يقوم البنك بتنفيذ بعض عمليات التحويل التي يقوم بها العميل والتي لا يوجد رصيد يغطيها (التحويل على المكشوف)، وذلك كشكل من أشكال الائتمان الذي يمنحه البنك لعميله، الأمر الذي لا يوجد في قواعد حوالة الحق المدنية ما يبرره.

وذهب البعض الآخر(2) للقول بأن الأمر يتعلق بإنابة كاملة، الآمر بالتحويل فيها هو المنيب والبنك هو المناب، والعميل المستفيد هو المناب لديه وهو ما يعنى أن الأمر يتعلق بتجديد الدين، وبناءً عليه تبرأ ذمة الأمر بالتحويل (المنيب) قبل المناب لديه (المستفيد) ليحل البنك محله في أداء هذا الدين عن طريق التحويل(3). ولكن عيب على هذا الرأي بأن التحويل المصرفي لا يستخدم فقط للوفاء بالديون بل قد يستخدم أيضا لإنشاء الديون ونقل النقود من طرف لآخر

---

(1) انظر هذه الآراء د. **على جمال الدين عوض**،مرجع سابق، ص١٨٩.

(2) انظر د. **على البارودي**، العقود وعمليات البنوك التجارية، دار المطبوعات الجامعية، ٢٠٠١، ص ٣١٠.

(3) المادة ٣٦٠ **فقرة** ١ من القانون المدني المصري.

(الواهب والمُوهب له، الوكيل والموكل)[1].

ويذهب الرأي الراجح فقها[2] وقضاء[3] بحق إلى القول بأن عملية التحويل المصرفي هي مجرد أداة لتداول المبالغ المقيدة في الحسابات المصرفية، نشأت في أحضان البنوك، وتطورت بفعل العرف المصرفي، وهو ما يحول دون إسنادها إلى نظم قانونية عرفها القانون المدني، وذلك نظرا للاختلافات الجوهرية بين هذه النظم وبين عملية التحويل المصرفي، ومن ثم يكون من الأوفق ترك عملية التحويل المصرفي ليحكمها العرف المصرفي باعتبارها نوعًا جديدًا من التعامل يصعب إخضاعه للنظم القانونية المعروفة في القانون المدني.

هذا وقد تبنى قانون التجارة رقم ١٧ لسنة ١٩٩٩ هذا الرأي؛ حيث تجنب إضفاء وصف قانوني معين على العلاقة بين البنك وعميله بخصوص عملية التحويل، وفضل أن ينظم العلاقة الاتفاق المبرم بينهما بخصوص عملية التحويل[4].

وبناء عليه يعد التحويل الإلكتروني للنقود عقد غير مسمى، يتمتع بطبيعة خاصة تستعصى على الخضوع لأحد القوالب القانونية المعروفة، ومن ثم يستمد أحكامه من اتفاق البنك والعميل.

---

(١) **د. عبد الفضيل محمد أحمد**، مرجع سابق، ص٤٧٤.

(٢) **د. حمدي عبد المنعم**، العمليات المصرفية، دار النهضة العربية، الطبعة الأولى، (بدون تاريخ نشر) ص٧٦، انظر أيضا **د.عبد الرحمن قرمان**، مرجع سابق، ص ٢٥٤.

(٣) **نقض مدني مصرى**، ١٤ /٦/ ١٩٦٧، طعن رقم ٢٩٤، س ق ٣١، القاعدة (١٩٢) مجموعة أحكام محكمة النقض،، س ١٨، ص ١٢٦٦.

(٤) **المادة ٣٢٩ الفقرة الثانية.**

٢- التزامات أطراف عملية التحويل الإلكتروني للنقود:

يتمخض عن التحويل الالكترونى للنقود بالمعنى السابق العديد من الالتزامات، منها ما يتحمله البنك الالكترونى، ومنها ما يتحمله العميل، وذلك على التفصيل التالى:

أولا/التزامات البنك الإلكتروني في مواجهة العميل الآمر بالتحويل:

٢٣١- يقع على عاتق البنك الإلكتروني مجموعة من الالتزامات في مواجهة العميل بموجب عقد التحويل الإلكتروني للنقود، أهمها تمكين العميل من إجراء التحويل عبر شبكة الانترنت، وإعلام العميل بكافة البيانات والارشادات الخاصة بعملية التحويل، وقيام البنك بتنفيذ أمر التحويل الصادر من العميل، وذلك على التفصيل التالي:

١- تمكين العميل من إجراء التحويل الإلكتروني عبر شبكة الإنترنت:

٢٣٢- يتصدر التزامات البنك تجاه عميله بخصوص تقديم خدمة التحويل الإلكتروني للأموال، التزام الأول بتمكين الثاني من التعامل مع نظام التحويل الإلكتروني عبر شبكة الإنترنت. وهذا الالتزام لم يكن موجودا في ظل نظام التحويل المقدم من قبل البنوك التقليدية، والذي كان يعتمد على تبادل الأوراق من خلال حضور العميل بصورة مادية في مقر البنك لطلب خدمة التحويل. لكن في ظل البيئة الإلكترونية التي يحيا البنك ويتعامل في كنفها، كان لابد أن يكون اتصال العميل بالبنك من ذات طبيعة هذه البيئة، الأمر الذي يفرض على البنك تمكين العميل من تحقيق هذا الاتصال، وذلك من خلال تزويد العميل بكافة

الأجهزة والبرامج التي تمكنه من التواصل مع البنك عبر شبكة الإنترنت[١].

وهذا الالتزام يتشابه مع التزام البنك بتمكين العميل من التعامل بالنقد الإلكتروني الذي سبق التعرض له بخصوص قيام البنك بإصدار النقد الإلكتروني، ومن ثم نحيل في خصوص تفاصيل هذا الالتزام إلى ما سبق ذكره في هذا الصدد[٢].

٢- الالتزام بإعلام العميل بتعليمات عملية التحويل:

٢٣٣- يعد التزام البنك بإعلام العميل بتفاصيل عملية التحويل من أهم الالتزامات التي يجب أن يقوم بها البنك في مواجهة عميله بخصوص عملية التحويل[٣]، ومبعث هذه الأهمية هي ما يتمتع به هذا الالتزام من خصوصية في ظل عمل البنك الإلكتروني العامل عبر شبكة الإنترنت، حيث يفرض التعامل عن بعد عبر وسيلة اتصال إلكترونية تعامل العميل مع البنك من خلال خطوات ذات طبيعة فنية، تتمثل في كيفية تشغيل مجموعة من الأجهزة والبرامج من أجل التواصل مع البنك بخصوص عملية التحويل، الأمر الذي يفرض على البنك إعلام العميل بهذه الخطوات، وذلك من خلال وضع إرشادات وتعليمات محددة تأخذ بيد العميل حتى تمام عملية التحويل. ويجب أن يراعى البنك الدقة في هذه التعليمات، وأن يضعها في مكان واضح على الموقع الإلكتروني الخاص به، وبطريقة سهلة

---

(1) **FCIC: Electronic Banking,** Electronic Fund Transfers ,Op. Cit., p.1

(٢) انظر سابقا، ص ٤٠٨.

(3) **Consumer rights in electronic fund transfers**, california department of consumer affairs division of legal affairs(Legal Guide CR-6): Op, Cit, p. 4, **The new Banking delivery system** (The Internet): Op. Cit, p. 2.

ومنظمة، بحيث يستطيع العميل أن يستوعبها(١).

هذا ولا يوجد في النظام القانوني المصري نصا ينظم التزام البنك العامل عبر شبكة الإنترنت بإعلام عميله بتفاصيل عملية التحويل.

أما عن الوضع في النظم القانونية الأخرى، فقد أولى المشرع الأمريكي أهمية كبيرة لنظام التحويل الإلكتروني للنقود، حيث أصدر قانونا ينظم هذه العملية بصورة مفصلة، وهو قانون التحويل الإلكتروني (EFTA regulation E)(٢)، حيث شدد هذا القانون على أهمية إعلام البنك عميله بكافة التفاصيل الخاصة بعملية التحويل الإلكتروني.

وعن أهم البيانات والإرشادات التي يجب على البنك الإلكتروني أن يزود العميل بها، فقد عرضت لها أحد عقود التحويل الإلكتروني للنقود على النحو التالي(٣):

أ- أن يحدد له البنك أنواع التحويلات الإلكترونية التي يمكن له القيام بها في ضوء رصيده، أو في ضوء الائتمان الذي يمكن للبنك أن يمنحه له، وحدود تكرار عملية التحويل، والكمية المسموح بها. وتكاليف عملية التحويل.

ب- أن يبين البنك للعميل الوسائل التي تمكنه من إخطاره (البنك) في حالة

---

(1) **HSBC**, internet banking terms and conditions, item (3), processing your instructions, Op. Cit.

(٢) هذا القانون متاح على العنوان الإلكتروني التالي:
http://www.fdic.gov/regulations/laws/rules/6500-3100.html

(3) **Fram Bureau Bank FSB**, FBB internet banking access agreement and electronic fund transfer act disclosure, Op. Cit.,

حدوث تحويل لأمواله بصورة غير مشروعة، وذلك بمنح العميل أرقام تليفونات أو عناوين البريد الإلكتروني التي يمكن من خلالها إخطار البنك بذلك.

ج- أن يحدد البنك للعميل حدود مسؤوليته (العميل) عن التحويل الإلكتروني غير المشروع أو غير المرخص به، وذلك كما لو أهمل العميل في المحافظة على أدوات الدخول لحسابه والتعامل فيه؛ كان ضيع بطاقة الوفاء أو الائتمان الخاصة به أو ضيع الرقم السري للدخول لحسابه أو سمح للغير باستعماله(١).

وهذا ما نظمه قانون التحويل الإلكتروني الأمريكي (EFTA) سالف الذكر، حيث ذهب إلى انتفاء مسئولية العميل عن عمليات التحويل غير المشروع إذا لم يخطره البنك بالوسائل التي تمكنه من الإبلاغ عن واقعة الفقد أو السرقة، وأن يبين له حدود مسئوليته عن ذلك بصورة مكتوبة، والأوقات التي يمكن له إبلاغ البنك خلالها(٢).

أ- يجب على البنك أن يخطر العميل بكل عمليات التحويل التي صدرت عنه وأن يمده بالوثائق والمستندات التي تثبت عملية التحويل، وذلك من خلال إرسال بيانات دورية عبر البريد الإلكتروني مثلا عن حالة حسابه وكل ما

---

(1) **Consumer rights in electronic fund transfers**, California department of consumer affairs division of legal affairs (Legal Guide CR-6): Op. Cit, p. 2; **Interagency council issues guidance on electronic financial services and consumer compliance**; Op. Cit, p. 3.

(2) **Consumer rights in electronic fund transfers**, California department of consumer affairs division of legal affairs(Legal Guide CR-6): Op. Cit, p. 2.

يطرأ عليه من جديد، وذلك حتى يستطيع العميل أن يتعرف على التحويلات التي قام بها، ويكتشف لو أن هناك تحويلاً غير مشروع قد حدث حتى يبلغ البنك به(1).

ب- يجب على البنك كذلك أن يوضح للعميل الطرق التي من خلالها يستطيع أن يتسلم رسائل البنك وإشعاراته، وكيف يسجل أي خطأ فيها والإجراءات الواجب عليه اتباعها في حالة اكتشاف مثل هذا الخطأ، والمدة القانونية التي يمكن للعميل خلالها القيام بإخطار البنك، والتي بعد انتهائها يمكن أن يفقد حقه في الإخطار، ومن ثم ضياع حقه.

ج- يجب على البنك أن يوضح حدود مسؤوليته للعميل، وذلك في حالة إذا حدث خطأ من جانب البنك في إجراء عملية التحويل، أو في حالة أن فشل في تحقيق ما طلبه العميل منه.

د- يجب على البنك أن يوضح للعميل الحالات التي يمكن له فيها أن يكشف فيها عن سرية البيانات أو المعلومات المتعلقة بحساب العميل أو خاصة بعمليات التحويل التي قام بها(2).

---

(1) **Jyske Bank**, JBPB, Net Bank user agreement, (EN)-2007; Op. Cit.

(2) **وقد نص المشرع المصري في قانون البنك المركزي والجهاز المصرفي والنقد رقم ٨٨ لسنة ٢٠٠٣ في المادة ٩٨** منه على أن للنائب العام أو لمن يفوضه من المحامين العامين الأول على الأقل من تلقاء نفسه أو بناء على طلب جهة رسمية أو أحد من ذوى الشأن، أن يطلب من محكمة استئناف القاهرة الأمر بالإطلاع أو الحصول على أية بيانات أو معلومات تتعلق بالحسابات أو الودائع أو الأمانات أو الخزائن المنصوص عليها في المادة السابقة أو المعاملات المتعلقة بها إذا اقتضى ذلك كشف الحقيقة في جناية أو جنحة قامت الدلائل الجدية على وقوعها .

٣- تنفيذ عملية التحويل الإلكتروني:

٢٣٤- يعد التزام البنك بتنفيذ التحويل هو الالتزام الرئيس في عملية التحويل الإلكتروني للأموال. وهذا الالتزام من جانب البنك الإلكتروني ينطوي على مجموعة من الالتزامات، وذلك على النحو التالي:

- الالتزام بالتحقق من شخصية العميل الآمر بالتحويل. والمقصود بهذا الالتزام تأكد البنك وتبينه من أن أمر التحويل الموجه إليه صادر عن عميله الذي له الحق فعلا في توجيه مثل هذا الأمر بموجب التعاقد الذي يحكم العلاقة بينهما(١). ويكتسب هذا الالتزام خصوصية في نظام عمل البنك الإلكتروني العامل عبر شبكة الإنترنت؛ وذلك بالنظر لطبيعة الوسيلة المستخدمة لتواصل العميل مع البنك، وهي شبكة الإنترنت، التي هي عبارة عن وسيلة للاتصال عن بعد، يغيب في ظل التعامل بها الحضور المادي لأطراف عملية التحويل، الأمر الذي يفرض على البنك ضرورة التحقق والتثبت من شخصية العميل الآمر بالتحويل حتى يقوم بتنفيذ التحويل.

وهناك العديد من الوسائل التي يمكن أن يعتمد عليها البنك للتحقق من شخصية الآمر بالتحويل، كالتوقيع الإلكتروني (Electronic signature)، أو كلمة المرور (password)، أو غيرها من الوسائل التي تساعد على التحقق من الشخصية(٢). ويجب على البنك أن يسلم هذه الوسائل لعميل، وأن يزوده بكافة

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 32

(2) **Thomas C. Glaessner, Tom Kellermann, Valerie McNevin**, Electronic safety and Soundness, Op,Cit, p 127; **consumer rights in electronic fund transfers**, california department of consumer

التعليمات والإرشادات اللازمة لاستخدامها، ومن ثم يجب على البنك أن يمتنع عن تنفيذ التحويل في حالة أن تبين له أن الأمر التحويل صادر عن شخص غير مخول له بذلك، بل تذهب بعض البنوك لأبعد من ذلك بالنص صراحة على امتناعها عن تنفيذ التحويل لو تبين أن الأجهزة والبرامج المستخدمة في توجيه الأمر لها غير تلك التي قامت بتسليمها للعميل(١).

وبناءً عليه يتحمل البنك المسؤولية كاملة عن أي انتقاص في حساب العميل تم بموجب عمليات التحويل صدرت من قبل شخص غير مخول له بذلك، مادام قد ثبت أن العميل التزم بتعليمات البنك بخصوص الحفاظ على الأدوات والبرامج المسلمة له لتوجيه أوامر التحويل للبنك(٢). ويتحمل البنك هذه المسؤولية حتى لو ثبت أنه لم يصدر عنه أي خطأ سواء عقدي أم تقصيري، وذلك تأسيسا على قواعد تحمل التبعة (نظرية تحمل المخاطر)، والتي تجعل البنك مسئولاً عن نشاطه الذي يتضمن بعض المخاطر حتى ولو لم يوصف هذا النشاط بأنه خاطئ. ولا يستطع البنك دفع مسؤوليته في هذه الحالة إلا بإثبات السبب الأجنبي(٣).

- الالتزام بالتأكد من كفاية المبالغ الموجودة في حساب الآمر بالتحويل لإتمام عملية التحويل(٤)، حيث يجب على البنك وهو بصدد تنفيذ أمر العميل أن يستطلع حالة الحساب الخاص به، والنظر في مدى كفايته لإجراء عملية

---

affairs division of legal affairs(Legal Guide CR-6): Op, Cit, p. 2.

(1) **HSBC**, internet banking terms and conditions, item (5), Op. Cit:

(2) Ibid.

(٣) **د. شريف محمد غنام**، مسؤولية البنك عن أخطاء الكمبيوتر في النقل الإلكتروني للنقود، مرجع سابق، ص١٠٣؛ انظر أيضا: **د. نوري حمد خاطر**، مرجع سابق، ص١٨١٥.

(4) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 32.

التحويل. فإذا كانت هذه المبالغ كافية، يجب عليه تلبية طلب العميل. أما إذا لم تكن هناك نقود في حساب العميل، أو كانت هناك، ولكنها لا تكفي لإتمام عملية التحويل فالأصل أن البنك يملك في هذه الحالة أن يرفض تنفيذ أمر العميل بالتحويل[1]. لكن ليس هناك ما يمنعه من تنفيذ الأمر (تحويل على المكشوف)، وذلك بدافع منح العميل ائتمانًا معينا (قرض)، على أن يقوم البنك بتحصيل هذه المبالغ من قبل العميل فيما بعد. ومنح العميل ائتمان بهذه الصورة قد ينظمها عقد التحويل الذي يجمع بين البنك والعميل، وذلك بأن يحصل العميل على موافقة البنك بتغطية عمليات التحويل التي يقوم بها حتى ولو كانت تتجاوز حدود المبالغ الموجودة في رصيده لدى البنك، وفي هذه الحالة يرجع البنك على العميل بهذه المبالغ بموجب العقد الذي يحكم العلاقة بينهما. وقد يقوم البنك بهذا الأمر من تلقاء نفسه كخدمة يقدمها للعميل بهدف كسب ثقته وتشجيعه على التعامل مع البنك، على أن يعود البنك على العميل بدعوى دفع غير المستحق أو الإثراء بلا سبب لتحصيل هذه المبالغ.

- نقل المبلغ المحول من حساب الآمر بالتحويل إلى حساب المستفيد. ويعد هذا الالتزام هو تمام تنفيذ البنك لعملية التحويل في مواجهة الأمر بالتحويل، وذلك لأن الأخير لا تبرأ ذمته في مواجهة المستفيد لمجرد إصدار الأمر بالتحويل

---

(1) (You" client" are responsible for making sure that there are sufficient funds on your account on the settlement days, otherwise the instructions cannot be excuted)

Jyske bank, JBPB, Net Bank user agreement, (EN)-2007; Op. Cit.

إلى البنك، ولكن بقيام البنك بنقل المبلغ من حسابه إلى حساب المستفيد. ونقل المبلغ المحول قد يتم داخل ذات البنك وذلك كما لو كان للمستفيد حساب لدى بنك الآمر بالتحويل، حيث يتم في هذه الحالة عن طريق القيد المزدوج في حساب الأمر بالتحويل (بالخصم)، وحساب المستفيد (الإضافة)، وقد يتم خارج بنك الآمر بالتحويل، وذلك في حالة ما إذا كان حساب المستفيد لدى بنك آخر. وفي هذه الحالة نفرق بين ما إذا كان التحويل بالإضافة (credit transfer)، أم بالخصم (debit transfer)، حيث في الحالة الأولى يقوم بنك الأمر بالتحويل بالمقاصة مع بنك المستفيد عبر شبكة الإنترنت لإضافة المبلغ في حساب المستفيد. أما في الحالة الثانية فأن بنك الأمر بالتحويل يقوم بخصم قيمة المبلغ المطلوب تحويله من حساب الأمر بالتحويل بناء على طلب بنك المستفيد الذي يقدم كافة المستندات (كالشيك الإلكتروني، أو الفاتورة الإلكترونية) التي تثبت مديونية الآمر بالتحويل للمستفيد[(١)].

هذا ولا يوجد نص خاص في النظام القانوني المصري ينظم التزام البنك بتنفيذ عملية التحويل الإلكتروني للنقود بالمعنى السابق، ومع ذلك يمكن القول بأن النصوص الواردة في قانون التجارة المصري رقم ١٧ لسنة ١٩٩٩ يمكن أن تستوعب هذا الالتزام مع مراعاة الطبيعة الإلكترونية لعملية التحويل، وما يفرضه ذلك من التزامات معينة. فقد نصت المادة ٣٢٩ على أن (النقل المصرفي عملية يقيد البنك بمقتضاها مبلغا معينا في الجانب المدين من حساب الأمر بالنقل بناء على أمر كتابي منه وفى الجانب الدائن من حساب الآخر).

---

(1) Ross **Cranston**, principles of banking law, Op, Cit, p. 235; **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 33

وعلى الرغم من أن صيغة المادة السابقة توحي بالتزام البنك بتنفيذ عملية التحويل، إلا أنه لا يراعى الطبيعة الإلكترونية لعملية التحويل التي يقوم بها البنك العامل عبر شبكة الإنترنت، والتي تفرض على البنك مراعاة هذه الطبيعة ضمن التزامه بتنفيذ أمر التحويل، والتي من أهمها التحقق من شخصية العميل الآمر بالتحويل، الأمر الذي يجب معه على المشرع المصري أن ينظم هذا الالتزام بالنص عليه بصورة صريحة مراعيا الطبيعة الإلكترونية لعملية التحويل التي يقوم بها البنك العامل عبر شبكة الإنترنت.

وعن الوضع في النظم القانونية الأخرى، فقد نظم قانون البنوك في كل من ألمانيا (BGB, art 242) [(١)] وفرنسا (CA Paris, 15th) [(٢)] التزام البنك العامل عبر شبكة الإنترنت بتنفيذ أمر التحويل الإلكتروني بالمعنى سالف الذكر، كما ذهب القانونان إلى التزام البنك الإلكتروني بتنفيذ عملية التحويل الإلكتروني للنقود بعناية وحرص (reasonable care and skill)، وأن يتحلى بحسن النية (good faith)، وذلك من خلال تنفيذ تعليمات العميل بخصوص هذه العملية، وتزويده بكل البيانات المتعلقة بها، وأن يقدم له كافة الوثائق التي توضح وتثبت عملية التحويل، على أن يقاس هذا الحرص بمعيار الشخص العادي في ذات الظروف، وهذا الالتزام يمتد ليشمل الوسطاء الفنيين الذين يتولون تنفيذ عملية التحويل.

---

(1) **Ross Cranston**, principles of banking law, Op, Cit, p. 235; **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 33; **diretto da M.J. Bonell**, Good Faith in German Law and in International Uniform Laws, Roma 1997, p 9. available at: w3.uniroma1.it/idc/centro/publications/ 24schlechtriem.pdf

(2) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 34.

وقد يفهم مما قرره كل من القانونين الألماني والفرنسي أن التزام البنك في تنفيذ أمر التحويل هو التزام ببذل عناية وليس بتحقيق نتيجة. ولعل المشرع في كل من البلدين أراد تبني المفهوم الجديد لبذل العناية في مجال التجارة الإلكترونية. فمعيار بذل العناية **due care** كوسيلة لقياس الالتزام قد شهد تطورا في معاملات التجارة عبر شبكة الإنترنت، حيث يحدد هذا الالتزام في ضوء المخاطر المرتبطة بالنشاط الذي يقوم به الملتزم، بما يفرض عليه تحليل المخاطر المتوقعة والمحيطة بالنشاط الملتزم به، ثم يجب عليه بذل عناية تتناسب مع حجم هذه المخاطر، يضاف إلى ذلك أن مقدار العناية المطلوبة يتحدد في ضوء النشاط، وليس كما كان من قبل في ضوء القائم بالنشاط (معيار الشخص العادي) [1].

وعلى الرغم من كل هذا، إلا أن ما يبدو لنا في هذا الصدد هو ضرورة أن يكون التزام البنك الإلكتروني بتنفيذ عملية التحويل التزامًا بتحقيق نتيجة، بحيث تنعقد مسؤوليته أمام العميل لمجرد عدم تحقق النتيجة المطلوبة. ولا يكفينا القول بمجرد التزام البنك ببذل عناية، وهذا ما يتفق مع طبيعة عقد التحويل، الذي يعد تنفيذ عملية التحويل فيه أمرًا متوقع الحدوث في ضوء الطبيعي من الأمور. وبناء عليه يكفي العميل للرجوع على البنك أن يثبت عدم تحقق هذه النتيجة، دون أن يكون مكلفًا بإثبات خطأ البنك في ذلك، ولا يستطيع البنك دفع مسؤوليته في هذا الخصوص إلا بإثبات السبب الأجنبي.

لكن السؤال الذي يطل برأسه علينا يتعلق بمدى حق البنك الإلكتروني في الامتناع عن تنفيذ أمر العميل بالتحويل، ونطاق هذا الحق.

---

(1) **Amity Yoran**; Op, Cit, p. 2.

٢٣٥- لم يجب قانون التجارة المصري ١٧ لسنة ١٩٩٩ على هذا التساؤل وهو بصدد تنظيم عملية النقل المصرفى.

ولم يظهر لنا معالجة هذا الأمر في التشريعات الأخرى التي عالجت التحويل الإلكتروني للأموال.

ومن خلال مطالعة نماذج عقود التحويل الإلكتروني للنقود الموجودة على مواقع البنوك العاملة عبر شبكة الإنترنت، تبين أن هذه البنوك تعطى لنفسها الحق في الامتناع عن تنفيذ أمر التحويل في حالات معينة، أهمها(1):

- إذا لم يكن للعميل نقود كافية في حسابه لإجراء عملية التحويل.
- إذا كان هناك إجراء قانوني يمنع أو يحظر على العميل أن يسحب من أموال من حسابه.

  إذا كان حساب العميل مغلقا أو مجمدًا.
- إذا كان التحويل يترتب عليه تجاوز العميل لحدود الائتمان الممنوح له من قبل البنك.
- إذا كانت الأداة أو الوسيلة الإلكترونية المستخدمة في عملية التحويل تعمل بشكل غير صحيح.
- إذا قام العميل بإدخال بيانات غير مكتملة أو غير صحيحة للبنك بخصوص عملية التحويل.

---

(1) **Hanmi bank,** Hanmi internet banking service agreement, Terms and Conditions, Paragraph B. scope of Liability, Op. Cit.

- إذا لم يتبع العميل التعليمات التي قدمها له البنك الإلكتروني لإجراء التحويل بشكل صحيح.
- إذا حدثت بعض الأمور التي تخرج عن حدود السيطرة كحريق، أو إجراء تحويل غير شرعي لوقوع أداة التحويل في يد شخص ليس له صفة.

ويجب على البنك أن يحيط العميل علمًا بكل هذه الحالات، وذلك في إطار التزامه بإعلام العميل ببيانات وتعليمات عملية التحويل، وذلك حتى يتجنب توجيه الأمر بالتحويل للبنك في مثل هذه الحالات.

وأخيرًا يثور التساؤل عن التزام البنك بعدم القيام بعملية التحويل، وذلك إذا قرر العميل الرجوع عن أمر التحويل.

٢٣٦- تعرض أحد البنوك العاملة عبر شبكة الإنترنت للاجابة عن هذا التساؤل فى نماذج عقود التحويل التى يقدمها، حيث فرق بين أمرين[١]:

الأول: حالة إن كان الأمر الصادر من العميل للبنك قبل تنفيذ التحويل، في هذه الحالة يجب على البنك أن يلبى طلب العميل في ذلك باعتبار أن النقود لم تخرج من حساب الآمر بالتحويل.

الثاني: إذا كان الأمر الصادر من العميل للبنك بعد تنفيذ التحويل، في هذه الحالة لا يملك البنك تنفيذها الأمر؛ وذلك باعتبار أن النقود قد خرجت من حساب الأمر بالتحويل، ولم يعد يملك التعامل عليها.

(1) **Jyske bank**, JBPB, Net Bank user agreement, (EN)-2007; Op. Cit.

لكن هذا لا يمنع العميل من إمكانية الرجوع على المستفيد بدعوى دفع غير المستحق، أو دعوى الإثراء بلا سبب إذا ما تبين له عدم أحقية المستفيد في هـذا المبلغ (كما لو قام بإصدار أمر التحويل على سبيل الخطأ).

ثانيا/ التزامات العميل الآمر بالتحويل في مواجهة البنك الإلكتروني:

٢٣٧- يقابل الالتزامات السابقة للبنك مجموعة من الالتزامات التي يجب علـى العميل التقيد بها في مواجهة البنك، وذلك على النحو التالي(١):

١- يأتي في مقدمة التزامات العميل تجاه البنك الإلكتروني الالتزام بسداد كافـة الرسوم والعمولات والمصاريف المختلفة المستحقة للبنك الإلكتروني نظيـر القيام بعملية التحويل الإلكتروني، وهذه المبالغ تشمل المقابل الذي يحـصل عليه البنك نظير تمكين العميل من استعمال الأجهزة والبرامج التي يستعملها الأخير في عملية التحويل، هذا بالإضافة إلى مصاريف عملية التحويل ذاتها. وعادة ما يقوم البنك بالحصول علي هذه المبالغ من خلال الخصم من حساب العميل. وفى حالة عدم وجود مبالغ في حساب العميل تغطى نفقات التحويل يمكن للبنك في هذه الحالة أن يوقف تنفيذ عملية التحويل حتى يحصل علـى المبالغ المستحقة له.

٢- ويجب على العميل أن يقوم باستلام كافة الوسائل التي يقـدمها لـه البنـك لاستخدامها في عمليات الدخول للحساب وإجراء التحـويلات الإلكترونيـة، كبطاقة الوفاء أو بطاقة السحب، أو البرنامج الذي يستخدمه من خلال جهاز

---

(1) **FCIC: Electronic Banking,** Electronic Fund Transfers, Op, Cit; **Hanmi bank,** Hanmi internet banking service agreement, paragraph D. Fees, Op, Cit.

الكمبيوتر الخاص به لإجراء عمليات التحويل. أيضا يجب عليه استلام الأرقام السرية الخاصة باستعمال هذه الأجهزة والبرامج[1].

٣- ويوصى العميل أن يقوم باختيار كلمة سر يصعب على أحد أن يتوقعها (فمثلا يكون الرقم الذي يختاره مختلفا عن رقم تليفونه أو رقم الأمن القومي الخاص به أو تاريخ ميلاده، على نحو يكون من الصعب فيه سرقة الرقم من قبل الغير) كما يجب عليه أن يراعى التغيرات التي قد يدخلها البنك على نظام الدخول على الحساب لاعتبارات أمنية يقدرها البنك. ويقتضي قيام العميل باستلام هذه الوسائل الحصول على كافة التعليمات الخاصة بتشغيلها، واختبار هذا التشغيل.

٤- يجب على العميل أن يلتزم بالمحافظة على كافة الوسائل التي يزوده البنك الإلكتروني بها لاستخدامها في عمليات التحويل، وكلمات السر الخاصة بها، وأن يكون على حذر عند تعامله مع التجار، بحيث يكونون محل ثقة، وألا يطلعهم على بياناته المصرفية إلا في الحدود اللازمة لإتمام عملية التحويل. كما يجب عليه ألا يرسل البيانات المصرفية الخاصة به عبر نظم البريد الإلكتروني العامة (general or public e-mail)، أيضا يجب عليه أن يحرص على عدم ترك جهاز الكمبيوتر الخاص به دون رقابة خاصة في حالة اتصاله بالبنك. وبناء عليه إذا حدث أن فقد العميل هذه الأدوات أو انتهكت سريتها، فأنه يقع عليه التزام بإخطار البنك الإلكتروني في أقرب

(1) **Consumer rights in electronic fund transfers**, California department of consumer affairs division of legal affairs(Legal Guide CR-6); Op. Cit, p. 1; **JYSKE BANK, Jyske bank**, JBPB, Net Bank user agreement, (EN)-2007; Op.Cit

وقت ممكن بواقعة الفقد أو السرقة، وذلك حتى يخلي العميل بعد ذلك مسؤوليته عن التحويل غير المشروع الذي يتم بهذه الأدوات(١).

وقد ألزم القانون الأمريكي للتحويل الإلكتروني للأموال (EFTA, 15 USC) الصادر عام ١٩٧٨ في المادة ٢٠٥ العميل بضرورة المبادرة بإخطار البنك فور علمه بفقد أو سرقة الأداة التي يعتمد عليها في توجيه أمر التحويل، بحيث تنعقد مسئولية العميل عن عمليات التحويل غير المشروع إذا تمت بعد يومين العمل التالي لعلمه بواقعة الفقد أو السرقة(٢).

ويبدو لنا أن هذه المدة كمهلة يمكن للعميل خلالها إبلاغ البنك بواقعة الفقد أو السرقة كبيرة، خاصة بالنظر لقدرة العميل على القيام بالإبلاغ بصورة أكثر سرعة عن طريق رسائل البريد الإلكتروني، أو الاتصال التليفوني، وفي أي وقت، حيث يفترض أن البنك يعمل على مدار اليوم، لذلك يكفي لو كانت هذه المدة يومًا واحدًا من تاريخ علم العميل بواقعة الفقد أو السرقة، وذلك حتى لا يكون في طول المدة إجحاف بحقوق البنك في ذلك.

لكن ماذا لو أهمل العميل في المحافظة على هذه الوسائل على النحو الذي تسبب في إجراء عملية تحويل غير مشروع باستخدام هذه الأدوات من قبل من استولى عليها؟

لقد سكت المشرع المصري عن معالجة هذا الفرض، لكن من خلال مطالعة

---

(1) **Apostolos Ath. Gkoutzinis**; Op. Cit, p. 37

(2) Request for Public Comment on a proposal to Revise the official staff commentary to regulation E (Electronic Fund Transfers); Op. Cit, p. 40062

النظم القانونية الأخرى تبين أن المجلس الخاص في بريطانيا (The Privy Council) قد تعرض لتنظيم هذا الأمر مقررا إعفاء العميل من كل مسئولية عن هذا التحويل. وقد علل موقفه هذا بأن البنك هو المسئول عن التحقق من صفة العميل، وإدارة كل ما يتعلق بعملية التحويل[١].

لكن محكمة الاستئناف البريطانية (CA) لم يكن هذا موقفها، حيث على الرغم من حرصها على تحمل البنك الجزء الكبير من المسؤولية في التأكد من صفة العميل، وصحة أداة التحويل المستخدمة إلا أن دورها ينتهي عند هذه الحدود، على أن يسأل العميل عن أي تحويل غير مشروع تسبب فيه بإهماله، وعدم محافظته على أداة التحويل المسلمة له[٢].

ونحن من جانبا ننضم إلى رأى محكمة الاستئناف البريطانية فيما ذهبت إليه؛ حيث لا يجب، تحت دعوات حماية المستهلك، الإثقال على كاهل البنك على النحو الذي يجعله مسئولاً حتى عن إهمال العميل وتقصيره في المحافظة على الأدوات المسلمة إليه لإجراء التحويل.

ولا يقبل القول بأن البنك مادام قرر الاستفادة من التكنولوجيا في تقديم الخدمات المصرفية فعليه أن يتحمل المسؤولية كاملة عن الأخطاء والمخاطر الناجمة عن هذا الاستخدام[٣]. فكما يستفيد البنك من التكنولوجيا في تقديم الخدمات المصرفية، يستفيد أيضا العميل في حصوله على الخدمة بطريقة سهلة

---

(1) **Graham Smith**; Op. Cit. p. 277.

(2) Ibid,

(٣) **د. شريف محمد غنام**، مسئولية البنك عن أخطاء الكمبيوتر في النقل الالكتروني للنقود، مرجع سابق، ص١٠٣.

وبسيطة، ومن ثم لا بد من توزيع المسؤوليات في هذا الخصوص بشكل عـادل ودون إجحاف بحقوق البنك. ولا يخل بهذا التوزيع العادل التشديد من مسئولية البنك بالنظر إلى أنه في مركز أقوى من العميل، لكن هذا لا يقبل القول بانتفاء مسئولية العميل تماما، فالبنك تمتد مسئوليته إلى ما يصدر عنه من أخطاء، وما يترتب عن نشاطه من مخاطر تؤدى إلى حدوث التحويل بصورة غير مشروعة، لكن إذا ثبت أن العامل الرئيس في ذلك هو خطأ وإهمال العميل فإنه المسئول في هذه الحالة.

هذا وقد عالج أحد العقود الخاصة بالبنوك العاملة عبر شبكة الإنترنت حالة الحساب المشترك (Joint account)؛ وذلك لو سمح أحد عملاء البنك لشخص معه بالتعامل مع البنك على الحساب الخاص به، حيث ألزم البنك العميل بتقديم البيانات الخاصة بهذا الشخص، وموافقة العميل الصريحة على إشراكه، كما ألزم العميل والمشترك معه في هذه الحالة أن يتعاملا مع البنك بكلمة سر واحدة[1].

٥- يجب على العميل أن يتوخى الحرص والعناية عند توجيه أمر التحويل للبنك، وذلك بأن يراعى صحة ودقة البيانات التي يبلغ البنك بها، وذلك في ضوء التعليمات والإرشادات التي يزوده البنك بها. وهذه البيانات تشتمل على البيانات الخاصة بشخص العميل، والبيانات الخاصة بحسابه، والمبلغ المطلوب تحويله، وأيضا البيانات الخاصة بالمستفيد من أمر التحويل، كما يلتزم بإخطار البنك الإلكتروني في حالة حدوث أي خطأ في إدخال هذه

---

(1) **Jyske bank,** JBPB, Net Bank user agreement, (EN)-2007; Op. Cit.

البيانات في أسرع وقت ممكن[١].

٦- يجب على العميل أن يفحص كافة الوثائق والإيصالات التي تصل إليه من البنك والخاصة بعمليات التحويل، ويحتفظ بها كي يقارنها بالبيان الدوري الذي يصل إليه من البنك، حتى يستطيع أن يكتشف أي خطأ أو نقص في عمليات التحويل، ومن ثم يتخذ الإجراءات التي تحفظ له حقه من الضياع[٢].

وإذا كان ما سبق ذكره هو أهم الالتزامات الواقعة على عاتق كل من البنك الإلكتروني وعميله بموجب العقد الذي ينظم العلاقة بينهما، فإن التساؤل يثور بشأن طبيعة العلاقة القانونية بين البنك الإلكتروني والمستفيد من التحويل، والتي يقوم البنك على أساسها بإضافة مبلغ التحويل في حساب هذا المستفيد؟

٢٣٨- الأصل أن المستفيد من التحويل الإلكتروني أجنبي عن العلاقة بين البنك الإلكتروني وعميله الأمر بالتحويل، وذلك ما لم يكن الآمر بالتحويل هو نفسه المستفيد (وذلك في الحالة التي يكون التحويل بين حسابين لشخص واحد)، ومن ثم نفرق بين ما إذا كان التحويل بين حسابين لشخصين مختلفين لدى ذات البنك، أم لشخصين مختلفين لدى أكثر من بنك، وذلك على النحو التالي:

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 34.

(2) **First Utah bank**, Electronic services agreement, P. 6. available at: http://www.Firstutah bank.com/internet_access.html.

أ- إذا كان التحويل الإلكتروني بين حسابين لشخصين مختلفين لدى ذات البنك:

٢٣٩- تتأكد الطبيعة القانونية الخاصة للتحويل الإلكتروني للنقود واستقلاله عن النظم القانونية المعروفة في القوانين التجارية والمدنية، والتأكيد على أنه من إبداعات الفن المصرفي، عند تحديد طبيعة العلاقة القانونية بين البنك الإلكتروني والمستفيد من أمر التحويل في هذه الحالة، حيث ينشأ للمستفيد في مواجهة البنك الإلكتروني حق مباشر ومستقل بمجرد القيد الفعلي في حسابه. وينشأ حق المستفيد هذا استقلالا عن العلاقة بين البنك والآمر بالتحويل؛ أي أن البنك الإلكتروني لا يستطيع أن يتمسك في مواجهة المستفيد بالدفوع التي كان يملك أن يتمسك بها في مواجهة الأمر بالتحويل والناشئة عن بطلان العلاقة الأصلية بين الأمر بالتحويل والمستفيد.

يضاف إلى ذلك، أنه إذا حدث ولم يكن الرصيد الخاص بالأمر بالتحويل يساوى قيمة المبلغ المراد تحويله، وقام البنك الإلكتروني على الرغم من ذلك بإجراء التحويل، فإنه لا يستطيع الرجوع عن هذا القيد اعتمادا على عدم كفاية الرصيد. بل يرجع على الأمر بالتحويل في هذه الحالة، وذلك على أساس أن الزائد على قيمة الرصيد يعد قرضا من البنك الإلكتروني للآمر بالتحويل، وذلك كله مع احتفاظ البنك الإلكتروني بحقه في عدم تنفيذ أمر التحويل إذا لم يكن الرصيد كافيا[١].

وبذلك يتضح أن التحويل الإلكتروني عملية مجردة عن سببها في العلاقة

---

(١) **د. حمدى عبد المنعم**، مرجع سابق، ص٦٨

بين البنك الإلكتروني والمستفيد من أمر النقل[١]. لكن كل هذا لا يعطل حق البنك الإلكتروني من ضرورة التأكد من صحة أمر التحويل الإلكتروني، وذلك من خلال التأكد من صدور الأمر عن العميل ذاته والذي له الحق في توجيه مثل هذا الأمر للبنك، وذلك عن طريق الوسائل التي تعين البنك على ذلك مثل التأكد من كلمة المرور أو التوقيع الإلكتروني الخاصين بهذا العميل، والتي عادة ما يحتفظ البنك بمثل هذه البيانات فيّ قاعدة البيانات الخاصة به، حتى يقوم بعملية المضاهاة على نحو دقيق. كذلك التأكد من شخصية المستفيد، وأنه صاحب الحق الشرعي في مبلغ التحويل، وإضافة المبلغ المحول في حسابه بعد التأكد من ذلك خاصة إذا كان أمر التحويل الصادر من العميل قد تم توصيله إلى البنك الإلكتروني عن طريق المستفيد (كما لو كان أمر التحويل قد صدر في صورة شيك إلكتروني يأمر من خلاله العميل البنك الإلكتروني بدفع المبلغ الثابت فيه للمستفيد حامل الشيك).

ويجب على البنك أن يستعين في ذلك بجهات التوثيق الإلكتروني التي تعينه على التعرف على شخصية من يتم التعامل معه بدقة، وبطرق متعددة[٢]. ويمكن القول إن البنك إذا أخل في التحقق من شخصية المستفيد على النحو الذي أدى إلى إجراء التحويل بصورة غير مشروعة فإن البنك يتحمل المسؤولية في هذه

---

(١) د. **عبد الرحمن قرمان**، مرجع سابق، ص ٢٥٠

(٢) د. **إبراهيم الدسوقي أبو الليل**، توثيق التعاملات الإلكترونية ومسئولية جهة التوثيق تجاه الغير المتضرر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي، ص١٨٥٣.

Apostolos Ath. Gkoutzinis; Op. Cit, p35. **Alain Hiltgen. Thorsten kramp. Thomas**; Op. Cit, p. 29.

الحالة تجاه الآمر بالتحويل بموجب العقد الذي يحكم العلاقة بينهما. وهذا ما نص عليه القانون الفرنسي من أن البنك يجب أن ينفذ عملية التحويل كما أمره الآمر بالتحويل، وطبقا للعقد الذي يحكم العلاقة بينهما بحيث يسأل البنك عن إهماله وتقصيره في ذلك[1] ولا شك أن عدم قيام البنك بالتحقق من شخصية المستفيد من التحويل هي أشد صور الإهمال من جانبه.

ب- إذا كان المستفيد من التحويل له حساب خارج البنك الإلكتروني:

٢٤٠- في هذه الحالة فإن البنك الإلكتروني بعد تلقيه أمر التحويل من الآمر بالتحويل، فإنه يقوم بالاتصال ببنك المستفيد إلكترونيا عبر شبكة الإنترنت ويطلب منه إجراء القيد في الجانب الدائن من حساب المستفيد بقيمة التحويل (يستوي أن يكون هو ذاته الآمر بالتحويل، أو شخصًا آخر) [2].

ويقوم بنك المستفيد بإجراء هذا القيد بصفته وكيلا من الباطن عن البنك الإلكتروني الأمر بالتحويل[3]. مع ملاحظة أن عميل البنك الإلكتروني الآمر بالتحويل له الحق في استعمال الدعوى المباشرة في مواجهة بنك المستفيد، وذلك إعمالا لأحكام الوكالة من الباطن التي نص عليها القانون المدني المصري[4]. وبناءً عليه يكون البنك الإلكتروني مسئولاً عن أعمال وكيله كما لو كان هذا العمل صادرا من البنك الإلكتروني نفسه متى لم يكن العميل الآمر بالتحويل قد أذن للبنك الإلكتروني أن يوكل غيره في إجراء عملية التحويل الإلكتروني

---

(1) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. 35.

(2) **Apostolos Ath. Gkoutzinis**; Op, Cit., p. 34.

(٣) **د. على جمال الدين عوض**، المرجع السابق، ص ١٥٩.

(٤) **المادة ٧٠٨ الفقرة الأولى والثانية.**

للأموال.

أما إذا كان العميل الآمر بالتحويل قد أذن للبنك الإلكتروني بأن يوكل بنكًا آخر في إجراء عملية التحويل ولم يحدد له بنكًا بعينه، فإن البنك الإلكتروني لا يكون مسئولاً إلا عن خطئه في اختيار نائبه، أو عن خطئه فيما أصدره له من تعليمات(١)، ويلاحظ أن تفويض عميل البنك الإلكتروني للبنك الإلكتروني في توكيل بنك المستفيد لإجراء عملية القيد في الحساب الدائن للمستفيد يستفاد ضمنا من صدور أمر التحويل الإلكتروني من العميل للبنك الإلكتروني حيث يحدد العميل للبنك فيه أسم البنك المستفيد.

٢٤١- وبعد تمام عملية التحويل الإلكتروني على النحو السابق ذكره، فإن هناك مجموعة من الآثار تترتب على النحو التالي:

- ففى العلاقة بين العميل الآمر بالتحويل والبنك الإلكتروني يترتب على تنفيذ عملية التحويل براءة ذمة البنك الإلكتروني في مواجهة العميل بمقدار المبلغ الذي تم تحويله، حيث يعد كما لو كان قد سحب هذا المبلغ من حسابه. لكن إذا كان البنك الإلكتروني قد قام بتنفيذ عملية التحويل الإلكتروني دون أن يكون للعميل رصيد يسمح، فإن البنك الإلكتروني يكون دائنا له بهذا المبلغ كما لو أنه أقرضه إياه.

- وفى العلاقة بين العميل الآمر والمستفيد، تبرأ ذمة الأول تجاه الأخير من

(١) ويتحقق هذا الفرض في حالة إذا ما استعان البنك الإلكتروني ببنك آخر لإجراء عملية التحويل الإلكتروني لعدم وجود حساب للبنك الإلكتروني المكلف بالتحويل لدى بنك المستفيد فيقوم البنك الإلكتروني في هذه الحالة بتوكيل بنك أخر يكون لديه حساب للبنك الإلكتروني ولبنك المستفيد لإجراء عملية التحويل. وهنا يكون كلا من البنك الإلكتروني ووكيله متضامنين في المسئولية في مواجهة العميل الآمر بالتحويل.

الدين الذي كان في ذمته لأن التحويل يعد وسيلة من وسائل الوفاء.

- أما في العلاقة بين البنك الإلكتروني والمستفيد فأن تنفيذ العميلة يترتب عليه اعتبار البنك الإلكتروني مدينا للمستفيد بقيمة المبلغ المحول، وهذه العلاقة مستقلة تماما عن علاقة البنك بالعميل الآمر بالتحويل[1].

---

(1) د. حمدى عبد المنعم

الباب الثالث

أمن البنك الإلكتروني على شبكة الإنترنت

٢٤٢- تشكل قضية الأمن في نظام عمل البنك الإلكتروني العامل عبر شبكة الإنترنت، وما يحيط بها من تهديدات ومخاطر المعوق الأكبر أمام اكتساب ثقة الأفراد في هذه البنوك[١] وتعاملهم معها[٢]. ويعود ذلك إلى طبيعة البيئة التي ينشأ

---

(١) د. حسين الماحي، نظرات قانونية في التجارة الإلكترونية، مرجع سابق، ص ٢٨٦

- جاء في دراسة مسحية أجرتها مجلة انترنت العالم العربي (ونشرت على جزئين) حول البنوك الإلكترونية، أن إحدى الدراسات التي أجرتها شركة eFunds (وهي شركة لتحويل الأموال الكترونيا تملكها مؤسسة deluxe corporation) تشير " إلى أن إنجاز الأعمال المصرفية على شبكة الانترنت، ما زال معقدا جدا، وأن الكثير من العملاء ما زالوا متخوفين من الناحية الأمنية. ويقول ماثيولاولر كبير المديرين التنفيذيين لشركة Online Resources، التي توفر الخدمات المصرفية الفورية لحوالي ٤٠٠ شركة في الولايات المتحدة : "إن حوالي ٣٦٥ شخصا منهم (٨٣ بالمائة) يقولون إن تعاملاتهم مع المصارف عبر الانترنت أفضل من تعاملاتهم مع المصارف التقليدية، ولكن المشكلة الأمنية كبيرة في حياة هذه البنوك، ويبدو أن هناك تذمرا على نطاق واسع بين المستهلكين، الذين يطالبون بتبسيط هذه الخدمات وتأمينها ".

انظر: **يونس عرب**، البنوك الإلكترونية، مرجع سابق:

Available at: http://www.arablaw.org/Download/E-Banking.doc.; **Susannah Fox and Jean Beier**, Op, Cit, p. 2; **Carl Pacini and others**, At the interface of the electronic frontier and the law: The international legal environment for systems reliability assurance services; Op. Cit, p.186.

(2) **Zakaria I.Saleh, Op, Cit, p.** 7; **Katyal, Neal Kumar,** Op. Cit. p. 39; **Adrian McCullagh and William Caelli**, Op, Cit, p. 338.

وقد أظهرت إحدى الدراسات التي قام بها معهد (Ponemon) في الولايات المتحدة الأمريكية عام ٢٠٠٦ أن عددا ممن يتعاملون مع البنوك الإلكترونية العاملة عبر

فيها هذا البنك ويؤدى خدماته وهي شبكة الإنترنت، والتي تتميز بكونها شبكة مفتوحة على العالم بأسره، لا توجد سلطة منفردة قادرة على التحكم فيها والسيطرة عليها[1]، ولا توجد قوانين موحدة رادعة تحكم الانتهاكات التي تستهدف أمن هذه الشبكة، الأمر الذي جعل لهذه القضية بعدا دوليا[2]. بل حتى على صعيد النظم الداخلية يوجد قصور تشريعي في مجال أمن المعاملات الإلكترونية في العديد من الدول خاصة النامية منها، مما دفع بالمجرمين إلى استغلال هذا القصور من خلال ارتكاب انتهاكاتهم الأمنية في دولة ما، عبر مؤسسات توجد في دولة أخرى[3].

يأتي ذلك في ظل التطور المستمر في مستوى مستخدمي الحاسوب، والمتعاملين مع شبكة الإنترنت في استخدام هذه الشبكة، مما أصبح يشكل تهديدًا

شبكة الانترنت وصل إلى حوالي ٤٤ مليون عميل وأن هذا العدد في زيادة مستمرة، وأن مسألة تامين وجود البنك وتعاملاته على شبكة الانترنت هي من أهم المسائل المؤثرة في نجاح هذه البنوك وذكرت الدراسة أن حوالي ٣٤% ممن يتعاملون مع هذه البنوك قد يتركون التعامل معها إذا حدث لأحدهم مشكلة أمنية واحدة، وأن حوالي ٥٤% منهم قد يتركون التعامل معها إذا حدث لهم مشكلتان أمنيتان.

Rob Rachwald, Op. Cit, p. 11

(1) **Zakaria I.Saleh**, Op. Cit, p. 7.

(٢) د. **محمد عبد الظاهر** حسين، المسؤولية القانونية في مجال شبكات الانترنت، مرجع سابق، ص ٨.

Scott F. Uhler, Philippe R. Weiss , Michele M. McGee, Liability issues and the internet part 1: Electronic mail, available at: http://www.lib.niu.edu/ipo/1996/il960266.html; http://www.itep.ae/arabic/EducationalCenter/CommNet/_security.asp

(3) **Thomas C. Glaessner, Tom Kellermann, Valerie McNevin,**; Op. Cit, p. 3.

كبيرًا بسبب امتلاك مجموعة من هؤلاء خبرة رصينة في التعامل مع المواقع الإلكترونية، ورغبة جامحة في استكشاف الجوانب الخفية منها، الأمر الذي سهل عليهم الدخول إلى نظم الشبكات المتخصصة، وفك رموز شفراتها الأمنية، والوصول إلى ما بها من معلومات، والعبث بها، واستغلالها لأغراض شخصية[١].

٢٤٣- كل هذه الأسباب دفعت العديد من الدول إلى محاولة تحصين مقدراتها الإلكترونية الموجودة على شبكة الإنترنت، خاصة البنوك العاملة عبر هذه الشبكة، وذلك من خلال توفير حماية لهذه المقدرات (المواقع الإلكترونية، الأجهزة المتصلة بالإنترنت)، وحماية للتعاملات التي تتم من خلالها. وقد ظهر أثر ذلك في الولايات المتحدة الأمريكية، حيث قامت المائدة المستديرة للمصارف (The Bankers Roundtable)[٢] باتخاذ قرار بإنشاء أمانة خاصة بالعمليات

(١) ا. **حسن مظفر الرزو**، الأمن المعلوماتي: معالجة قانونية أولية، مجلة الأمن والقانون، أكاديمية شرطة دبي، السنة الثانية عشر، العدد الأول، يناير ٢٠٠٤، ص٦٨؛

- **Apostolos Ath. Gkoutzinis**, Op, Cit, p. 149;**David L. Baumer and others;** Op. Cit, p. 407;**John Carlson, Karen Furst, William W.Lang, Daniel E.Nolle**; Op. Cit, p. 18.

(٢) تمثل المائدة المستديرة (**BITS**) المصارف الوطنية الرئيسة في الولايات المتحدة الأمريكية، حيث تضم في عضويتها أكثر من ١٢٥ مؤسسة مالية، كما تضم في عضويتها الجمعيات المصرفية الوطنية. وتعمل هذه المائدة على تزويد المصارف في الولايات المتحدة وفروعها حول العالم بحلول للقضايا الأمنية الخاصة بالعمليات المصرفية، عمليات التشفير، السرية، والتوثيق. وفي عام ١٩٩٦، أصدرت دليلا يضم مجموعة من المبادئ الخاصة بقضايا السرية في المصارف وذلك للوصول إلى موقف موحد بينهما في هذا الخصوص. انظر

Alfred M. Pollard, Hearing on electronic authentication and digital signature, Senate banking, housing and Urban Affairs committee, available at:

المصرفية الإلكترونية تحمل اسم أمانة صناعة تقنيـة المـصارف (Banking Industry Technology Secretariat)، حيث يأتي في مقدمة أهدافها العمـل على توفير الحماية الأمنية للبنوك العاملة على شبكة الإنترنت، من خلال التركيز على قضايا التكنولوجيا، والعمل على توفير كل ما تحتاج إليه هذه البنـوك مـن برامج وأدوات للدخول، وكافة صور الحماية الأمنية الممكنة.

ولا شك في أن الأمر جد خطير، فهي مسألة مرتبطة بوجود البنـك علـى شبكة الإنترنت من عدمه، الأمر الذي يحتاج منا إلى التعرف على كل ما يرتبط بمفهوم أمن البنك الإلكتروني، وصور الانتهاكات التي يمكن أن يتعـرض لهـا، والوسائل التقنية والحلول القانونية الكفيلة لمواجهة هذه الانتهاكات، لذلك سنقـسم هذا الباب إلى فصلين، نتعرف في الفصل الأول على المقـصود بـأمن البنـك الإلكتروني، وصور الاعتداءات التي يمكن أن يتعرض لها والتوثيق الإلكتروني باعتباره آلية الحماية الممكنة. وفى الفصل الثاني نعرض للمـسؤولية القانونيـة الناشئة عن انتهاك أمن البنك، سواء بالنسبة للمعتدين، أم بالنسبة لجهة التوثيـق، وذلك على النحو التالي:

---

http://www.senate.gov/~banking/97_10hrg/102897/witness/pollard.htm

الفصل الأول

ماهية أمن البنك الإلكتروني وصور الاعتداءات التى تستهدفه

٢٤٤- سبق أن ذكرنا الأهمية القصوى للأمن في نظام البنوك العاملة عبر شبكة الإنترنت سواء على صعيد وجود البنك، أم على صعيد معاملاته، الأمر الذي يدعو إلى التعرف على مفهوم واضح للمقصود بأمن البنك الإلكتروني على شبكة الإنترنت، وصور وأشكال الانتهاكات التي يمكن أن يتعرض لها، وذلك من أجل الوصول إلى فهم صحيح ورؤية واضحة لطبيعة هذه المشكلة والإحاطة بكافة أبعادها، حتى يتسنى لنا الوقوف على معالجة قانونية سليمة لهذه المشكلة في ضوء طبيعة البنك وتعاملاته. لذلك سنقسم هذا الفصل إلى مبحثين، الأول للحديث عن ماهية أمن البنك على شبكة الانترنت، والثاني لصور الاعتداءات التي يمكن أن يتعرض لها البنك، وذلك على النحو التالي:

المبحث الأول

ماهية أمن البنك على شبكة الإنترنت

٢٤٥- بداية، تجدر الإشارة إلى أن النظام القانوني المصري يخلو من وضع تعريف لما يقصد بأمن البنك العامل عبر شبكة الإنترنت، ولا حتى مفهوم الأمن الإلكتروني على شبكة الإنترنت بصورة عامة. فعلى الرغم من أن قانون تنظيم التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤ صدر لينظم استخدام التوقيع الإلكتروني كوسيلة لتأمين وإثبات المعاملات الإلكترونية، إلا أنه غفل عن وضع تعريف للأمن الإلكتروني.

وعلى الرغم من أنه ينصح دائما بابتعاد المشرع قدر الإمكان عن وضع التعريفات، إلا أنه يفضل أن يستعاض عن ذلك بصياغة أسس يقوم عليها هذا المفهوم، وذلك بغرض توضيح وإبراز الفكرة، خاصة إذا ما كانت من الحداثة بمكان، وذلك كما فعلت بعض التشريعات مثل قانون التحديث المالي **(Financial Modernization Act)** الصادر في الولايات المتحدة الأمريكية سنة ٢٠٠١ [١]، حيث لم يضع مفهوما محددا لما يقصد بأمن البنك الإلكتروني، ولكنه وضع أسسًا ومعايير يتم من خلالها تحديد هذا المفهوم[٢].

وفي ظل هذا الصمت التشريعي المصاحب لأهمية وضع تعريف لأمن البنك على شبكة الإنترنت، يدعونا الأمر إلى محاولة إيجاد تأصيل فقهي لهذا المفهوم،

---

(١) هذا القانون متاح على العنوان الإلكتروني التالي:

http://banking.senate.gov/conf/summ.pdf

(2) **Anita K. Pennathur**; Op. Cit, p. 2118.

وذلك في ضوء الطبيعة الخاصة للعمليات المصرفية، والطبيعة الخاصة للبيئة الإلكترونية(شبكة الإنترنت) التي تحيا هذه البنوك في كنفها.

٢٤٦- ويثير وضع تعريف لأمن البنك الإلكتروني العامل عبر شبكة الإنترنت صعوبات خاصة، تتمثل في:

(١) حداثة فكرة أمن البنك الإلكتروني العامل عبر شبكة الإنترنت؛ حيث لم تعترف كثير من التشريعات، خاصة العربية منها، بالتعامل عبر شبكة الإنترنت إلا منذ فترة قريبة، وحتى هذه التشريعات لم يصل بها الحال إلى التعرض لأمن البنوك العاملة على هذه الشبكة. أيضا التشريعات الأوربية التي عالجت هذا الأمر عالجته من منظور الأمن الإلكتروني بصورة عامة. يضاف إلى ذلك ندرة الأحكام القضائية في هذا المجال. بل يمكن أن نقول أيضا قلة الدراسات القانونية في هذا الخصوص.

(٢) خصوصية أمن البنك الإلكتروني العامل على شبكة الإنترنت. فالتشريعات القانونية تسعى جاهدة إلى تأمين التعاملات الإلكترونية على شبكة الإنترنت، بالنظر إلى أهمية هذه التعاملات، وبالنظر إلى شبكة الإنترنت المحاطة بالعديد من المخاطر. فالسعي يزداد الجهد فيه بالنسبة للبنوك العاملة على هذه الشبكة، وذلك بالنظر لخصوصية البنوك وتعاملاتها المصرفية، والتي تعظم فيها فكرة الأمن، وبالنظر إلى أهمية وخطورة هذه التعاملات، وما تحتويه من معاملات مالية وأسرار مصرفية، تحتاج إلى أن يفرد لها أحكام أمنية خاصة.

(٣) اختلاف أمن البنك الإلكتروني عن أمن البنك التقليدي[١]، وهـذا الاخـتلاف مبعثه سيطرة الوسائل الإلكترونية على وجود البنك الإلكتروني وتعاملاته، مما أدى إلى اختلاف صور المخاطر التي يمكن أن يتعرض لهـا البنـك، واختلاف وسائل الحماية، الأمر الذي انعكس على تحديد مفهوم هذا الأمن.

وفي ظل هذه الصعوبات لم يكن هناك من سبيل سوى النظر لأمن البنك من منظور فكرة الأمن الإلكتروني على شبكة الإنترنت بصورة عامة، وذلـك فـي محاولة لتقريب الخطى لمفهوم واضح لأمن البنـك الإلكترونـي علـى شـبكة الإنترنت.

٢٤٧- والملاحظ على التعريفات التي عالجت الأمن الإلكتروني على شـبكة الإنترنت أنها تناولته من جانب معين، وتغافلت عن جوانب آخري، وذلك علـى النحو التالي:

أولا: التعريف التشريعي:

يخلو النظام القانوني المصري من تعريف محدد للأمن الإلكترونـي، كمـا أن معظم النظم القانونية التزمت الصمت حيال هذا الأمر، ولـم يظهـر لنـا مـن تشريعات تعرضت لتعريف الأمن الإلكتروني سوى قانون الصفقات الإلكترونية السنغافوري[٢] حيث عرفه بأنه "عبارة عن مجموعة الإجراءات التي تتم بغرض:

---

(1) **Katyal, Neal Kumar**; Op. Cit, p. 35.

(2) **Electronic transactions ACT 1998**, Legal guide to the electronic transactions ACT, available at: www.ida.gov.sg/doc/Policies%20and%20Regulation/Policies_and_Regulation_Level3/Legal_Guide_1998.pdf

- التأكد من أن السجل الإلكتروني صادر عن شخص معين.
- اكتشاف أي خطأ أو تعديل يطرأ على عملية الاتصال، أو محتوى السجل الإلكتروني.

ويتم ذلك من خلال استخدام لوغاريتمات أو رموز أو أرقام تعريف، أو تقنيات تشفير، أو أي أدوات أمنية مشابهة، من أجل التأكد من سلامة السجل الإلكتروني بالطرق الإلكترونية".

والملاحظ على هذا التعريف أنه تبنى رؤية ضيقة لمفهوم الأمن الإلكتروني على شبكة الإنترنت، حيث قصره على مجرد تأمين المعاملات الإلكترونية التي تتم عبر هذه الشبكة، متغافلة أمن الأجهزة والأدوات المستخدمة في هذه المعاملات. فالانتهاك الأمني يمكن أن يحدث من مجرد الدخول غير المشروع على أحد المواقع الإلكترونية أو الأجهزة المرتبطة بشبكة الإنترنت، حتى ولو لم يكن هناك معاملة قد تمت من خلال هذا الموقع أو هذه الأجهزة.

ثانيا/ التعريف الفقهي:

انقسم الفقه في سبيل تعريفه للأمن الإلكتروني إلى اتجاهين، على النحو التالي:

- الاتجاه الأول:

نظر أنصار هذا الاتجاه للأمن الإلكتروني من زاوية تأمين المعاملات الإلكترونية التي تتم عبر شبكة الإنترنت ضد بعض صور الانتهاكات التي يمكن أن تخل بهذا الأمن، فعرفوه بأنه عبارة عن "السياسات والتعليمات والإجراءات المتطلبة لإجراء الصفقات الإلكترونية في ظل أقل مستوى من مخاطر الانتهاك

أو الاختراق أو السرقة"[١].

والملاحظ على هذا الاتجاه أن أنصاره تبنوا ذات الرؤية الخاصة بقانون الصفقات الإلكترونية السنغافوري سالف الذكر، حيث حصروا فكرة الأمن الإلكتروني في مجرد تأمين المعاملات الإلكترونية التي تتم عبر هذه الشبكة، ومن ثم يوجه لهم ذات النقد، من تغافلهم عن أمن الأجهزة والأدوات المستخدمة في هذه المعاملات.

- **الاتجاه الثاني:**

ذهب أنصار هذا الاتجاه إلى النظر للأمن الإلكتروني من زاوية تأمين الأدوات والأجهزة التي تتم التعاملات الإلكترونية من خلالها، كالمواقع والشبكات الخاصة، حيث ذهبوا إلى أنه عبارة عن "الأدوات والبرامج التي تعمل على المنع أو الحد من الدخول غير المرخص إلى المناطق المحمية"[٢].

وعرفه البعض أيضا بأنه عبارة عن عملية تهدف إلى حماية نظم المعلومات من الوصول أو الاستعمال أو الاطلاع أو التعديل غير المرخص[٣].

وعلى الرغم من أن هذا الاتجاه قد تناول فكرة الأمن الإلكتروني من جانب بالغ التأثير وهو ما يتعلق بأمن الأجهزة والأدوات المستخدمة في التعامل

---

(1) **Thomas C. Glaessner, Tom Kellermann, Valerie McNevin,** Op. Cit, p. 8.

(٢) هذا التعريف متاح على العنوان التالي :

http://www.apt.gc.ca/dProdExpandE.asp?Id=513

(٣) انظر في هذا التعريف العنوان التالي:

http://www.answers.com/tOpic/information-security?cat=technology

الإلكتروني، إلا أنه أغفل جانبًا آخر يحتل أهمية مماثلة، وهي تأمين المعاملات الإلكترونية التي تتم عبر هذه الأدوات، وذلك لتمتعها بالاستقلال في مواجهة الأجهزة والأدوات، فتقليد موقع إلكتروني مماثل للموقع الذي يؤدى خدمة ما يؤدى إلى حدوث إخلال أمنى بالمعاملات الإلكترونية التي تتم، على الرغم من عدم المساس بأمن الأجهزة والأدوات الخاصة بالموقع المقلد.

٢٤٨- نخلص من ذلك إلى أن كلا من الاتجاهين عرض لمفهوم الأمن الإلكتروني على شبكة الإنترنت من جانب واحد وأغفل الجانب الآخر. فالأمن الإلكتروني ذو مفهوم واسع يشتمل على كل من أمن الأدوات ونظم المعلومات، وأيضا التعاملات والصفقات التي تتم من خلال هذه الأدوات والنظم. وهذا ما أوضحه جانب من الفقه(١)، عند تعرضه لفكرة الأمن الإلكتروني بخصوص تأمين البنك العامل عبر شبكة الإنترنت، حيث ذهب إلى أن هذا التأمين يتم على مرحلتين:

الأولى: تأمين المعاملات الإلكترونية التي تتم بين البنك وعميله، وما يقتضيه ذلك من تأمين المراسلات المتبادلة فيما بينهما ضد كافة الأشكال الاعتداء عليها.

الثانية: تأمين مقر البنك على شبكة الإنترنت، وما يقتضيه ذلك من حماية الأجهزة والبرامج التي تحتوى على البيانات الخاصة بالبنك.

لذلك يبدو لنا تعريف الأمن الإلكتروني على شبكة الإنترنت بأنه عبارة عن "حماية وتأمين الاجهزة والأدوات الإلكترونية، وما يتم عن طريقها من تعاملات وصفقات إلكترونية على شبكة الإنترنت من كافة أشكال التهديدات الأمنية".

---

(1) **Sofia Giannakoudi**; Op. Cit. p. 209.

وبما أن أمن البنك الإلكتروني على شبكة الإنترنت صورة من صور الأمن الإلكتروني على هذه الشبكة بصورة عامة، فأنه سوف يدور في فلك التعريف السابق مع بعض الإضافات التي تراعى خصوصية أمن البنك الإلكتروني على هذه الشبكة، والتي تتمثل في:

١- خصوصية محل الحماية، وهو البنك الإلكتروني ومعاملاته المصرفية، وذلك على النحو الذي يظهر معه مفهوم الأمن بصورة أكثر صرامة وفي أعلى درجات الحذر والاحتياط؛ باعتبار أن البنوك ومعاملاتها تزداد معها مبررات الأمن، من سرية المعاملات المصرفية وخصوصيتها، خاصة إذا ما كانت تتم عبر شبكة إلكترونية مفتوحة للاتصال عن بعد كشبكة الإنترنت.

٢- خصوصية المتعامل مع البنك، فالاعتبار الشخصي الذي تتأسس عليه المعاملات المصرفية يعكس أهمية تحديد هوية المتعامل مع البنك بصورة دقيقة، خاصة أن التعامل يتم عن بعد وبدون حضور مادي للمتعاملين.

لذلك نرى تعريف أمن البنك الإلكتروني العامل على شبكة الإنترنت بأنه عبارة عن تأمين الشبكة الداخلية للبنك وموقعه الإلكتروني علي شبكة الإنترنت، وتأمين كافة الخدمات المصرفية التي يقدمها بداية من التعرف على شخصية المتعامل وحتى حصوله على الخدمة المصرفية، وذلك ضد كافة أشكال التهديدات الأمنية.

والسؤال الذي يلقى بظلاله بعد التعرف على مفهوم أمن البنك الإلكتروني على شبكة الإنترنت يتعلق بطبيعة الفرق بين أمن البنك التقليدي وأمن البنك الإلكتروني الذي يعمل على شبكة الإنترنت.

من خلال التدقيق في التعريف السابق يتجلى لنا أن هذا الفرق يتركز في أمرين(1):

الأول: طبيعة محل الحماية. فهي في البنوك التقليدية عبارة عن أصول مادية من مباني وخزائن حديدية وأوراق ومستندات، تحتاج إلى مجموعة من أفراد الأمن المجهزين بمجموعة من الأسلحة أو أدوات الأمن الأخرى لحماية الموجودات المادية داخل مبنى البنك، سواء تمثلت هذه الموجودات في أموال أم أوراق خاصة بالتعاملات المصرفية للبنك. لكن الأمر مختلف تماما عند الحديث عن محل الحماية بالنسبة للبنك الإلكتروني العامل على شبكة الإنترنت(2)، حيث إن محل الحماية الأساس هو المعلومات المخزنة في الأجهزة والمتداولة عبر الموقع الإلكتروني. فعلى حد تعبير بعض الفقه(3). أن هذه البنوك ما هي إلا نشاط مكثف من المعلومات، يتضمن معالجة للبيانات المالية والشخصية في داخل البنك الإلكتروني، وتوزيع خارجي لهذه البيانات في مواجهة العميل أو جهة الرقابة أو نظم المقاصة والتسوية.

الثاني: يتمثل في طبيعة البيئة التي يتم فيها النشاط المصرفي. فالبنوك التقليدية تعمل في المحيط المادي الملموس، أما البنوك الإلكترونية فهي تتواجد وتعمل عبر شبكة الإنترنت، والتي تتميز ببعض الخصائص التي تنعكس على مفهوم الأمن الخاص بهذه الشبكة وما يجرى فيها من تعاملات، وهذه الخصائص هي:

---

(1) **Zakaria I.Saleh;** Op, Cit, p. 6; **Andy Jones**; The convergence of physical and electronic security, Computer Fraud& Security, Volume 2006, Issue 3, March 2006, Pages 12-14.

(2) **Zakaria I.Saleh;** Op, Cit, p. 6; **Andy Jones**; Op. Cit, p. 12-14.

(3) **Apostolos Ath. Gkoutzinis**;Op, Cit, p. 179; **Shaoyi Liaoa and other**; Op. Cit, p. 63.

١- شبكة الإنترنت نظام مفتوح(١)، يستطيع أي شخص من خلال الاتصال بهـا أن يصل إلى أي شيء معروض على الشبكة(٢)، وأن يتعامل معه ما لم يكن هذا الشيء قد توافرت له نظم الأمن التي تحفظ عليه سريّته وخصوصيته(٣). فالبيانات تنتقل عبر هذه الشبكة بسهولة وانسيابية من دولة لدولة ومن منظمة لمنظمة، ومن فرد إلى مؤسسة دون قيود وبكل اللغات، وأثناء هذا الانتقـال تنتقل المعلومة في العديد من مناطق الاختصاص القضائي ومناطق السيادة،

---

(١) **د. إسماعيل شاهين**، أمن المعلومات في الانترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون (جامعة الإمارات العربية المتحدة)، ٢٠٠٠، ص ٧

Thomas C. Glaessner, Tom Kellermann, Valerie McNevin; Op, Cit, p. 1

(٢) وعلى الرغم من أن هذه السهولة في الحركة والتعامل تعد ميزة، إلا انها لا تخلو على الرغم من ذلك من العيوب والتي تتمثل في:

- أن انتقال البيانات عبر شبكة الانترنت يعتمد على بروتوكولات خاصة للتعامل مع المواقع ونقل البيانات والتي تسمى بروتوكولات عناوين الانترنت (**Internet Protocol address**)، حيث تتمثل نقطة الضعف في هذا البروتوكول في أن التعامل من خلاله يفرض على الأطراف معرفة أسم وعنوان الموقع، في الوقت الذي يعتمد فيه أمن الموقع على الاسم والعنوان الخاصين به، حيث إن هذا الضعف يمكن أن يستخدم كمدخل لاعتراض(**intercept**) ولتقليد(**Spoofing**) مجموعة البيانات والتطبيقات الخاصة بالتعاملات عبر الشبكة.
- الأمر الثاني، عدم قدرة هذا البروتوكول على معالجة سهولة الحركة والانتقال إلى الموقع، الأمر الذي لا يوفر حصانة كافية ضد الدخول السريع وغير الآمن. انظر في تفصيل ذلك:

Richard H. Paine, Secure mobile architecture (SMA– A way to fix the broken Internet),information on security technical Report, Vol 12, Issue 2, 2007, Pages 85-89

(٣) **د. إسماعيل شاهين**، مرجع سابق، ص ٧

Carl Pacini and others; Op. Cit, p. 188.

والكثير من هذه المناطق لا يكون بينها تعاون قانوني يمكن من خلاله التصدي للاعتداءات التي تستهدف سرية وخصوصية هذه البيانات، الأمر الذي يعظم من أهمية التأمين الذاتي، من خلال الاستعانة بالوسائل الفنية والتكنولوجية القادرة على توفير مناخ أمنى ملائم، يعمل على تكملة النقص الذي يعتور النظم القانونية سواء على الصعيد المحلى والدولي في هذا الخصوص.

٢- صعوبة تحديد هوية الشخص الذي يتم التعامل معه عبر شبكة الإنترنت، وذلك بسبب غياب الحضور المادي للأطراف أثناء إجراء التعاملات، وإجراء المعاملات عن بعد، الأمر الذي أوجد مشكلة تتعلق بتعرف كل متعاقد على شخصية المتعاقد الآخر، من خلال التحقق من هويته وأهليته القانونية اللازمة لإجراء التصرفات القانونية، وخلو إرادته من كل العيوب التي يمكن أن تشوبها، خاصة وأن هذا الأمر يحتل أهمية خاصة في المعاملات المصرفية، في ضوء الاعتماد الكبير على الاعتبار الشخصي للعميل. كل ذلك كان الدافع وراء ظهور هيئات حكومية تقوم بدور الوسيط بين المتعاملين، من خلال تعريف كل متعاقد على الآخر، والتوثق من جدية التعاقد(1)، على نحو ما سنبين لاحقا.

٣- إدراك أن المواقع على شبكة الإنترنت ذات قدرة كبيرة على التجميع والبحث والارتباط بالمصادر المتعددة للمعلومات على هذه الشبكة، فهي كما يطلق

(1) **Joris Claessens- Valentin Dem- Danny De Cock-Bart Preneel- Joos Vandewalle**; Op. Cit, p. 259; **Joris Claessens- Valentin Dem- Danny De Cock-Bart Preneel- Joos Vandewalle**; Op, Cit, p. 259.

عليها شبكة عنكبوتيه أطرافها متصلة ومترابطة فيما بينها، وهــذه القــدرة الفائقة تشكل ميزة كبيرة دفعت إلى احتدام الصراع للسيطرة علــى شــبكة الإنترنت، من خلال السعي للهيمنة على أسماء النطاقات وعناوين المواقع، والتنافس على سوق استضافة المواقع عبر الخوادم التقنية، والتوجه أحيانًــا للتحكم بالمعلومات، وطرق تبادلها من خلال السيطرة على الحلول التقنيــة واحتكارها للتحكم بمصائر المستخدمين. لكن في مثل هــذه القــدرة علــى التجميع والارتباط، خلقت تحديات أمنية كبيرة، حيث جعلت أمن أحد المواقع على الشبكة مرتبطا غالبا بأمن المواقع الأخرى(١)، الأمر الذي يفرض وجود حذر شديد من التعامل مع مواقع مجهولة وغير موثقة(٢).

٤- غياب سلطة مركزية قادرة على تحمل مسئوليات انتهاك السرية، وصــور الاعتداءات الأخرى التي تستهدف المواقع الإلكترونيــة علــى الــشبكة(٣). فالوضع الطبيعي في أي دولة أنها تملك أن تصدر تشريعا ينظم شيئا مــا، وتكفل فاعلية هذا التنظيم، نظرا لما تملكه هذه الدولة من وسائل الــسيطرة والسيادة، ووجود الجهات القادرة على الرقابة ومنع الاعتداء أو اســتمراره، والتي تتيح أيضا التعويض وملاحقة المخالفين. لكن في بيئــة الإنترنــت لا تتوفر سلطة مركزية ولا جهة سيادة توفر الحماية او تتيح الفرصة أو المكنة

---

(1) **David L. Baumer and others**; Op. Cit, p. 401.

(٢) لقد شهدت شبكة الانترنت تطورات واسعة النطاق مما دفع بالعديد من المجرمين إلى استغلال هذا التوسع وما يصاحبه من ترابط بين أطراف الشبكة المترامية في ارتكاب العديد من الجرائم. انظر:

Adrian McCullagh and William Caelli;Op, Cit, p. 339.

(3) **Nicholas Imparato**; Op. Cit, p. 15.

للحماية القانونية عند حدوث الاعتداء، فهي كما يعبر بعض الفقه(١) عنها بيئة يملكها كل شخص، وغير مملوكة لأحد.

وقد انعكست أوجه الاختلاف السابقة على صور الاعتداءات التي تستهدف أمن هذا البنك، ومن ثم على صور الحماية ضد هذه الاعتداءات على نحو ما سنبين لاحقا(٢).

والسؤال: ما هو نطاق مفهوم أمن البنك الإلكتروني؟ وهل هذا النطاق مقصور فقط على موقع البنك على شبكة الإنترنت أم أنه ذو نطاق أوسع من ذلك؟

٢٤٩- لاشك في أهمية هذا التساؤل، باعتباره يلقي مزيدا من الضوء على مفهوم أمن البنك على شبكة الإنترنت، وذلك لأنه يدعو لمعرفة المحاور التي يقوم عليها هذا المفهوم، ومن ثم معرفة أهداف الاعتداءات الأمنية، ووسائل الحماية.

ويمكن القول بأن مفهوم أمن البنك العامل على شبكة الإنترنت يقوم على ثلاثة محاور، والتي يجب أن تكون بمثابة أهداف لأي تنظيم قانوني يسعى إلى توفير بيئة آمنة لوجود وعمل البنك الإلكتروني على شبكة الإنترنت، ويحظى بثقة المتعاملين معه(٣) وهي:

---

(١) يونس عرب، دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي، منشورات اتحاد المصارف العربية، ٢٠٠٢، ص ١٨.

(٢) انظر لاحقا، ص ٥٢٤، ٦١٤.

(3) **Carl Pacini and others**; Op. Cit, p. 189; **Jennifer Iser**; Op, Cit, p. 50; **Fethi Calisir- Cigdem Altin Gumussoy**; Op. Cit, p. 216; **Background report on electronic commerce 1998**, Electronic commerce task force, 1998, p 162

١ - سرية البيانات (Privacy of Data):

ويقصد بسرية البيانات في نظام عمل البنك العامل عبر شـبكة الإنترنـت، حفظ البيانات من الاطلاع عليها من غير الأشخاص المخول لهم بـذلك، سـواء البيانات المخزنة في أجهزة البنك، أم التي يتم إرسالها عبر شبكة الإنترنت أثناء التعاملات المصرفية [١].

ولا شك في أهمية السرية بهذا المعنى باعتبارها إحدى الركائز القوية التي يتأسس عليها أمن البنك الإلكتروني[٢]، وذلك بالنظر إلى ما تهدف إليه من منـع التعرف على محتوى البيانات المحفوظة لدى البنك أو المعاملات المصرفية أثناء إبرام العقود الخاصة بها أو أثناء تداولها بين البنك والعميل بما تحتويه من بيانات

---

(١) د. إلياس الهاجرى، جرائم الانترنت،ص١ مقالة على شبكة الانترنت متاحـة علـى العنوان التالى:

http://www.egovs.com/egovs_webo2/news.php?main=7&detailsid=28

(٢) رافت رضوان، مرجع السابق، ص ٧٩.

Background report on electronic commerce 1998; Op. Cit p. 23.

David L. Baumer and others; Op. Cit, p. 400

وقد تصمنت التوجيهات الأوربية على هذا المعنى بخصوص المعاملات التي تتم عبر شبكة الانترنت بصورة عامة:

(The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet Open new possibilities for users but also new risks for their personal data and privacy)

Directive 2002/58/EC, Official Journal of the European Communities,12 July 2002, item (6)

مصرفية يحرص القانون أشد الحرص على سريتها[1].

هذا وقد عالج قانون التحديث المالي الأمريكي سالف الذكر هذا الأمر، وأظهر اهتماما شديدا بقضايا السرية المتعلقة ببيانات البنوك العاملة عبر شبكة الإنترنت، حيث تطلب من هذه البنوك ضرورة تبنى معايير ملائمة تتعلق بالحفاظ على البيانات الخاصة بالمتعاملين معها، والاستعانة بضوابط أمنية قوية في هذا المجال[2].

٢- سلامة المعلومات (Information Integrity):

يقصد بسلامة المعلومات حماية المعلومات المحفوظة أو المرسلة ضد كافة محاولات تغييرها بالحذف أو بالإضافة أو بالتعديل، بشكل متعمد أو غير متعمد إلا من قبل الأشخاص المخول لهم ذلك[3].

ولا شك في أهمية هذا الاعتبار الذي يهدف إلى الحفاظ على محتوى رسائل البيانات التي تمثل حقوق والتزامات البنك والمتعاملين معه بشكل مفيد وموثوق به[4].

---

1) **Electronic banking group initiatives and white papers**; Op. Cit, p. 20; **Carlos Martin& Denis Beau**; Op. Cit, p. 15.

2) **Anita K. Pennathur**; Op. Cit, p. 2118; **E-Banking,** Federal financial institutions examination council; Op. Cit, p. 14.

(٣) د. **إلياس الهاجرى**، المرجع السابق، ص١.

(٤) مقالة بعنوان **تحديات الأمن**، متاحة على شبكة الانترنت على العنوان التالي:
http://www.itep.ae/arabic/Education1Center/CommNet/net_security.asp

٣- التحقق من هوية الأطراف (Peer Authentication):

عرفت الدائرة الاتحادية بمحكمة الاستئناف الأمريكية تحقيق الهوية بأنه عبارة عن التأكد والتحقق من شخصية المتعامل بالاعتماد على بياناته الشخصية كالاسم والعنوان ورقم الضمان الاجتماعي، أو بالاعتماد على الخصائص البيومترية؛ كاتساع حدقة العين، والطول الموجي للصوت(١).

وتهدف هذه العملية إلى التأكد من هوية الأطراف المعنية بعمليّة تبادل المعلومات، حيث يجب على كل من البنك الإلكتروني والعميل أن يتأكد كل منهما من شخصية الآخر، وذلك لتجنب أي شكل من أشكال الخداع (مثل انتحال الشخصية)(٢).

وتتجلى أهمية هذه العملية كإحدى الدعائم القوية التي يقوم عليها أمن البنك بالنظر إلى ما تتميز به المعاملات المصرفية على شبكة الإنترنت من كونها عمليات تتم عن بعد؛ أي بدون حضور مادي لأطراف المعاملة، الأمر الذي يفرض لتأمين هذه المعاملات ضرورة تعرف كل طرف على هوية الآخر قبل التعاقد بخصوص الخدمات المصرفية(٣).

وقد تناول المحاور السابقة تقرير مبادئ إدارة المخاطر المتعلقة بالبنك

---

(1) **United States Court of Appeals for the Federal Circuit**, Decision-ing.com, 2007-1277, p. 21.

(2) **Joris Claessens- Valentin Dem- Danny De Cock-Bart Preneel-Joos Vandewalle**, Op. Cit, p. 259.

(3) **Authentication in an Internet Banking Environment**, Federal financial institutions examination council, available at: http://www.ffiec.gov/pdf/authentication_guidance. pdf

الإلكتروني (Risk Management Principles for Electronic Banking) الصادر عن لجنة بازل في يوليو ٢٠٠٣، حيث جاء فيه أربعة عشر مبدأ خاصًا بإدارة المخاطر المتعلقة بالبنك الإلكتروني. وقد ورد في المبدأ الثامن منه التأكيد على ضرورة "ضمان سلامة بيانات المعاملات المصرفية الإلكترونية، وما يرتبط بها من سجلات ومعلومات"[١].

وقد عبر عن هذه المبادئ قانون التحديث المالي الأمريكي سالف الذكر في المادة ٥٠١ منه، حيث نص على ضرورة تبنى البنك الإلكتروني معايير أمن مناسبة، وذلك من خلال الاستعانة بمجموعة من الإجراءات والأدوات، التي تسعى إلى الآتي:

١- تحقق أمن وسرية السجلات الخاصة بالعميل، وكافة ما يرتبط بها من معلومات.

٢- توفير الحماية ضد أية تهديدات متوقعة تستهدف سلامة هذه السجلات.

٣- توفير الحماية ضد كافة أشكال الدخول أو الاستعمال غير المشروع لهذه السجلات.

كما أن الدليل الخاص بهذا القانون تضمن بعض الاقتراحات التي يجب أن

---

(١) وقد تبنى هذا التقرير مجموعة من المبادئ التي تسعى إلى مواجهة المخاطر التي قد تعترض عمل البنوك الإلكترونية، وكيفية مواجهتها والتخفيف من حدتها، وذلك من خلال وضع سياسات للرقابة والتدقيق، وفرض التزامات بالعناية، وتنظيم قواعد المسئولية عن الإخلال في هذا الصدد. انظر:

Thomas C. Glaessner, Tom Kellermann, Valerie McNevin; Op. Cit, p. 40.

تؤخذ في الاعتبار من قبل البنك الإلكتروني وهى[1]:

أ- ضرورة تحديد وتقييم المخاطر التي ربما تهدد أمن البنك الإلكتروني.

ب-تبنى خطة مكتوبة تحتوى على سياسات وإجراءات للتحكم في هذه المخاطر.

ج- إجراء تعديل دوري لهذه الخطة على نحو يجعلها تراعى كل التغيرات التكنولوجية الجديدة، وكيفية التصدي لكافة أشكال التهديدات الداخلية والخارجية للمعلومات.

أما فيما يتعلق باقتصار نطاق مفهوم أمن البنك العامل على شبكة الإنترنت على موقعه الإلكتروني فقط فهو قول غير دقيق. فعلى الرغم من الأهمية البالغة لهذا الموقع باعتباره النافذة التي يطل من خلالها البنك على المتعاملين معه، والتي يمكن من خلالها النفاذ إلى النظم الداخلية للبنك[2]، إلا أن البنك له شبكة إلكترونية داخلية تنظم حركة العمل المصرفي على هذا الموقع، وهذه الشبكة عبارة عن مجموعة من الأجهزة والمعدات التي تتواجد في البيئة المادية، الأمر الذي يتطلب أيضا حماية هذه الشبكة بالطرق التقليدية للحماية المادية. لذلك نرى أن مفهوم أمن البنك الإلكتروني هو عملة ذات وجهين، أحدهما شبكة البنك الإلكتروني (بيئة تقليدية)، والآخر للمعاملات المصرفية الإلكترونية التي تتم عبر موقع البنك على شبكة الإنترنت (بيئة إلكترونية).

وبعد استعراض مفهوم أمن البنك الإلكتروني على النحو السابق ذكره، نلاحظ أن البيئة التي يوجد فيها البنك (شبكة الإنترنت)، كانت ذات تأثيرًا بالغ على

---

(1) Ibid, Op, Cit, p. 43.

(2) **Zakaria I. Saleh**; Op, Cit, p. 7.

مفهوم أمنه؛ وقد ظهر هذا الأثر على عناصر هذا المفهوم ومحـــاوره ونطاقـــه ومن ثم سيكون له أثر على صور ونوعية الاعتداءات التي تستهدف أمن البنك. ومن ثم صور الحماية المتطلبة على نحو ما سنعرض له في المبحثين القادمين.

المبحث الثاني

صور الاعتداءات على أمن البنك الإلكتروني

٢٥٠- تتعدد صور الاعتداءات والانتهاكات التي تستهدف أمن البنك العامل على شبكة الإنترنت، وتتجدد وتتنوع الوسائل التي تنفذ من خلالها هذه الاعتـــداءات. ويقف وراء ذلك، الطبيعة الخاصة لشبكة الإنترنت من ناحية، والطبيعة الخاصة للمعاملات المصرفية من ناحية آخري. فشبكة الإنترنت شبكة إلكترونية للاتصال عن بعد، تتسم بالتطور المستمر، وتحوى الكثير من الإبهام والغمــوض، الـــذي ينمى الرغبة لدى العديد من رواد الشبكة- حتى من غير المجرمين- إلى محاولة كشف هذا الإبهام والغموض، حتى ولو كان الأمر ينطوي على ارتكاب جريمة، وذلك بدافع التحدي للاستكشاف والمعرفة. وقد ساعدهم على ذلك سهولة التنقــل عبر المواقع الإلكترونية المختلفة على شبكة الإنترنت، وسهولة إرسال البيانـــات واستقبالها الأمر الذي يهدد أمن المعاملات الإلكترونية على هذه الشبكة بـــصورة عامة، وأمن البنك بصورة خاصة. يضاف إلى ذلك طبيعة المعاملات المصرفية، والتي تزداد بشأنها البواعث على الاعتداء؛ وذلك بالنظر إلى الطبيعة المالية لهذه المعاملات، الأمر الدافع إلى تنويع الأساليب والوسائل المتبعة للاعتداء على البنك ومعاملاته.

ويؤكد ذلك كله أهمية أمن البنك على شبكة الإنترنت، ويدعو للتعرف على أهم صور الاعتداءات التي تستهدف أمن البنك والمسؤلية القانونية عنها، وذلـــك على النحو التالي:

المطلب الأول

تقليد موقع البنك الإلكتروني على شبكة الإنترنت

(Spoofing Web Bank)

٢٥١- يعد تقليد الموقع الإلكتروني للبنك على شبكة الإنترنت من أهم وأخطر الاعتداءات التي يمكن أن تحدث للبنك وأكثرها شيوعا[١]، مما يدعو إلى التعرض لهذا الاعتداء من خلال تعريفه، وكيفية إكتشاف البنك لوقوعه، والاحتياطات التى يجب على العميل اتخاذها، والاجراءات الوقائية التى يجب على البنك الالتـــزام بها، والمسؤلية عنها، وذلك على التفصيل التالى:

١- التعريف بتقليد موقع البنك:

٢٥٢- وتتمثل هذه الصورة في محاولة المعتــدى (Intruder) تقليــد الموقـــع الإلكتروني للبنك على شبكة الإنترنت، في ذات التصميم، وبحمل ذات الشعارات وعدد الصفحات، وأن ينشيء به ذات الروابط، وذلك على نحو يظهر معه الموقع المقلد وكأنه الموقع الحقيقي للبنك الإلكتروني (shadow copy)[٢]. ويلاحظ أنه

---

(١) ويعد هذا الفعل من أكثر الأفعال خطورة وانتشارًا على شبكة الانترنت، حيث ذهــب مكتب التحقيقات الفيدرالية الأمريكي إلى أن ضحايا هذه الجريمة تقدر بالآلف يوميــا، كما انه طبقا لتقرير جهاز الأمن الأمريكي ولجنة سان فرانسيسكو للجرائم الإلكترونية فإن حوالي ٣٠ واقعة لتقليد المواقع تحدث كل يوم.

Neil Chou and others, Client-side defense against web-based identity theft, stanford university, Stanford CA 94305, (without publishment date), p 1

(2) **Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach,** Web spoofing: an internet, Technical report 540-96(Revised Feb.1997), P 3; **Zakaria I.Saleh;** Op, Cit, p. 8; **Yougu Yuan and**

لا يشترط أن يظهر الموقع المقلد مماثلا ومطابقا للموقع الحقيقي، بل يكفي أن يتسبب الموقع المقلد في إحداث خلط أو لبس لدى العملاء على نحو يدفعهم للتعامل معه على أنه الموقع الحقيقي للبنك، وذلك كما لو قام المعتدى بتقليد العناصر الأساسية المميزة لموقع البنك كعلامته التجارية، أو اسمه التجاري:

٢٥٣- ويسعى المعتدون لهذا العمل لتحقيق أحد غرضين:

- الرغبة في مراقبة التعاملات المتبادلة بين البنك الإلكتروني والعميل، وذلك من خلال الاطلاع على كل الرسائل التي يقوم العميل بإرسالها للبنك الإلكتروني لمجرد انتهاك سريتها والاطلاع على خصوصيات العميل(١).

- أو الرغبة في استغلال البيانات (Utilization Data) المتبادلة بين البنك والعميل، حيث إن الأخير بعد أن ينخدع في هذا الموقع الوهمى يقوم بالدخول عليه والتعامل معه كما يتعامل مع الموقع الحقيقي للبنك، فيدخل البيانات الخاصة به كاسم المستخدم وكلمة السر وأرقام بطاقة الائتمان، وأي بيانات أخرى خاصة بالتعامل مع الموقع الإلكتروني للبنك، ثم يقوم المعتدون بعد ذلك باستغلال هذه البيانات للتعامل مع حسابات هؤلاء العملاء على نحو يحقق مصلحة المعتدى ويضر بالعميل(٢).

---

others, Web Spoofing 2001, available at: www.cs.dartmouth.edu/pkilab/demos/spoofing/

(1) **Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach**; Op, Cit, p. 4.

(2) **Threat from Fraudulent Bank Web Sites**, OCC bulietin, Comptroller of the currency administrator of national banks, July 1, 2005. p1.available at:

٢- كيفية اكتشاف البنك الإلكتروني تقليد موقعه على شبكة الإنترنت:

٢٥٤- تبدو أهمية التعرض لكيفية اكتشاف البنك لتقليد موقعه على شبكة الإنترنت، في بيان الطرق التي يمكن من خلالها للبنك أن يكتشف هذا الأمر، وذلك من أجل تسهيل مهمته في ذلك، كما أن البنك يخضع في التزامه بمراعاة هذه الأمور لإشراف جهة الرقابة.

وتوجد بعض المؤشرات والدلائل التي يمكن من خلالها للبنك الإلكتروني اكتشاف وجود تقليد أو محاكاة لموقعه على شبكة الإنترنت، والتي تتلخص في قيام البنك بممارسة نوع من الرقابة على البيانات التي تأتى إليه، وتلك التي تخرج منه، ومن خلال البحث المستمر على الإنترنت عن المواقع غير القانونية أو غير المرخص لها في استعمال اسم البنك أو علامته التجارية، وذلك على النحو التالي:

- عودة رسائل إلكترونية (E-mail messages) إلى خادم رسائل البنك، لم ترسل أصلا من قبل البنك، حيث إن حدوث مثل هذا الأمر إشارة إلى أن رسائل إلكترونية وصلت للعميل باسم البنك، ومن ثم قام بالرد عليها. وفي بعض الحالات تحتوى هذه الرسائل على وصلات (links) مرتبطة بالمواقع المقلدة.

- مراجعة سجل خادم المواقع بصورة دورية ومنتظمة، حيث يمكن أن يبوح هذا السجل بعناوين لمواقع تتضمن اسم البنك الإلكتروني، أو عناوين لمواقع

---

http://www.occ.treas.gov/ftp/bulletin/2005-24.txt
Michael P. **Dierks**; Op. Cit, p. 311.

تحمل مقاطع مقاربة من مقاطع العنوان الإلكتروني الخاص بالبنك على شبكة الإنترنت مشكوك فيها، أو إلى أي نشاط غير مشروع آخر قد حدث.

- وجود زيادة في عدد الرسائل المرسلة من العميل لمركز أو لموظفي البنك، أو الاتصال المباشر للابلاغ عن وجود موقع مقلد[1].

٣- الاحتياطات الواجب على العميل الالتزام بها:

٢٥٥- تبدو أهمية التعرض لهذه الاحتياطات، باعتبارها التزامات يجب على العميل الالتزام بها عند قيامه بالتعامل مع الخدمات المختلفة لشبكة الإنترنت للوصول إلى موقع البنك الإلكتروني، وغالبا ما يقوم البنك بإدراج هذه الاحتياطات في كافة العقود التي تحكم علاقته بالعميل، لإلزامه بها بصورة قانونية، وذلك باعتبارها ترسم السياسة العامة للتعامل مع البنك عبر شبكة الإنترنت:

- يجب على العميل عدم التسرع في الرد على الرسائل التي تصل إليه إلا بعد أن يتأكد أنها قادمة من البنك الإلكتروني فعلا، وأن ينتبه إلى أن البنك غالبا لا يقوم بإرسال رسائل يطلب فيها تأكيد أرقام الحساب الخاص بالعميل مثلا (confirmation of account details).

- يجب على العميل أن يتوخى الحرص عند قيامه بكتابة عنوان البنك الإلكتروني (Web Site Address) في خانة المتصفح الخاصة بالعناوين

---

(1) Threat from Fraudulent Bank Web Sites; Op, Cit, p. 2; Yougu Yuan and others, Web Spoofing 2001, available at: www.cs.dartmouth.edu/pkilab/demos/spoofing/

الإلكترونية، وأن يقوم بالتأكد أكثر من مرة من صحة العنوان قبل أن يعطى الأمر بالدخول.

- يجب على العميل أن ينتبه إلى احتمال وجود مواقع إلكترونية وهمية على شبكة الإنترنت، بحيث لا يبادر بالتعامل مع الموقع لمجرد الشكل الظاهرى له، وأن ينتبه جيدا للعلامات المزيفة التي قد تستخدم للخداع.
- يجب على العميل التأكد قبل إدخال بيانات خاصة بحسابه من وجود مستويات تأمين خاصة بعمليات التشفير (Secure Sockets Layer)، ويجب على العميل أن يتأكد من أن القفل المغلق الخاص بالتشفير يعمل، فلو أنه قام بالضغط على القفل فإنه سيطلع على شهادة الموقع الخاصة بالبنك الإلكتروني، ومن ثم يستطيع التأكد من حقيقة الموقع[1].

٤- الإجراءات القانونية الواجب على البنك الإلكتروني اتباعها:

٢٥٦- يقصد بالإجراءات القانونية التي يجب على البنك اتباعها، الوسائل القانونية السريعة التي تستهدف الإيقاف الفوري للاعتداء.

وفي الواقع لا يوجد في النظام القانوني المصري نص خاص يرسم للبنك الإجراءات التي يجب أن يتبعها لإيقاف مثل هذا الاعتداء. ويأتي ذلك القصور في ظل الأهمية القصوى لهذه الإجراءات؛ باعتبارها وسائل فورية يمكن عن

---

(1) **Threat from Fraudulent Bank Web Sites;** Op, Cit, p. 2; **Yougu Yuan and others**, Web Spoofing 2001, available at: www.cs.dartmouth.edu/pkilab/demos/spoofing/ **Website Spoofing,** available at: http://strategis.ic.gc.ca/epic/site/cvbpr-cvbi.nsf/en/h_wd00162e. html; **Tips for Safe Banking over the Interne**, Federal reserve bank of New York ; Op. Cit, p. 1.

طريقها ايقاف هذا الاعتداء الذي يستنزف أموال العملاء من خلال استغلال كلمات المرور وأرقام الحسابات الخاصة بهم. كما يضر أيضا بالسمعة التجارية للبنك.

ومن خلال استطلاع الوضع في النظم القانونية الأخرى، وجد أن مكتب الرقابة على النقد الأمريكي (OCC) قد عالج هذا الفرض، وذلك عندما نص في أحد التقارير التي يصدرها على بعض الخطوات التي يجب على البنك العامل على شبكة الإنترنت اتخاذها في مثل هذه الحالة، وهى(١):

أ- يجب على البنك الإلكتروني أن يبادر بالاتصال بصورة فورية بمزود خدمات الإنترنت المسئول عن استضافة موقع الويب المزيف. ويطلب منه إغلاق هذا الموقع.

ب-الاتصال فورا بالجهة المسئولة عن تسجيل العناوين الإلكترونية على شبكة الإنترنت(Domain Names) والتي يدخل هذا العنوان في نطاق اختصاصها، ويطلب منها تعطيل استخدام العنوان المقلد (domain name disablement of the) نظرا لأحقية البنك في استخدام هذا العنوان. وعلى البنك في هذه الحالة أن يقدم لهذه الجهة ما يثبت تسجيله لهذا العنوان(٢).

---

(1) **Threat from Fraudulent Bank Web Sites**; Op. Cit, p. 3.

(٢) حيث كما سبق أن ذكرنا تسجيل العناوين الإلكترونية على شبكة الانترنت يحكمه مبدأ الأسبقية في التسجيل. والذي يعنى أن الأحقية في العنوان الإلكتروني تكون لمن كان له السبق في تسجيله لدى الجهات المختصة بذلك. وهذا المبدأ يعد بمثابة الشرط الوحيد لتسجيل الموقع. حيث يكاد ينحصر دور الجهة التي تتلقى طلبات التسجيل في مجرد التأكد من عدم سبق تسجيل العنوان المراد تسجيله لشخص آخر. انظر في تفصيل ذلك د. **شريف محمد غنام**، حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان

ج- يجب على البنك أن يبلغ السلطات المختصة، كي تقوم بتوجيه مذكرة إحضار (subpoena form) إلى من قام بتقليد موقعه، وذلك لاسترداد المعلومات الخاصة بالعملاء، والتي حصل عليها نتيجة قيامه بتقليد موقع البنك على شبكة الإنترنت[١]، وذلك طبقا لأحكام قانون حماية حقوق المؤلف الرقمية الأمريكي (The Digital Millennium Copyright Act of 1998)[٢]، ويعطى هذا القانون للبنك الحق أيضا في طلب مصادرة الخادمات (confiscation of servers) الخاصة بمن قام بتقليد موقع البنك، والتي ربما تحتوى على معلومات خاصة بحسابات العملاء.

ويبدو أن الإجراءات السابقة الهدف من ورائها فقط منع هذا النشاط غير المشروع الذي يقع على الموقع الإلكتروني للبنك، بحيث يبقى أمام الأخير الفرصة لمواجهة أصحاب الموقع المزيف أو المغشوش بأفعالهم الإجرامية التي ألحقت به الضرر، وذلك من خلال ملاحقتهم قضائيا على الصعيدين الجنائي والمدني لجبر هذا الضرر.

الإلكتروني، مرجع سابق ص١٦.

(1) **Threat from Fraudulent Bank Web Sites**; Op. Cit, p. 3.

(٢) وينص هذا القانون الخاص بتنظيم حقوق المؤلف الرقمية، والصادر في سنة ١٩٩٨ رقم (USC 512(h 17) على السماح لأي شركة تم تقليد موقعها على شبكة الانترنت، بأن تستصدر مذكرة إحضار إدارية من أي محكمة أمريكية مختصة محليا، كي توجه لأي مزود خدمة انترنت للكشف عن هوية أي مشترك لديها، والذي قام بصورة غير مشروعة بتقليد الاسم أو العلامة التجارية الخاصة بهذه الشركة. راجع هذا القانون على الموقع الإلكتروني التالي:

www.copyright.gov/legislation/dmca.pdf

٥- المسئولية القانونية لمقلد الموقع الإلكتروني للبنك:

٢٥٧- لاشك أن تقليد الموقع الإلكتروني للبنك العامل على شبكة الإنترنت يعد نشاطا غير مشروع من شأنه أن يلحق الضرر بالبنك وعملائه، مما يدفعنا للتساؤل عن مسئولية المعتدى عن هذا النشاط في مواجهة كل من البنك الإلكتروني وعملائه.

وتقتضى الإجابة عن هذا التساؤل التعرض لمسؤولية المعتدى في مواجهة كل من البنك والعملاء، وذلك على النحو التالي:

أولا: مسئولية مقلد الموقع الالكترونى للبنك:

٢٥٨- بالنظر إلى طبيعة نشاط المعتدى تجاه البنك يلاحظ أنه يشكل جريمة، حيث يقوم المعتدى بتقليد موقع البنك بغرض الإضرار بالبنك ونشاطه المصرفي على شبكة الإنترنت. لذلك يدعو الأمر إلى التعرف على المسؤولية الجنائية والمدنية للمعتدى تجاه البنك، وذلك على النحو التالي:

(أ) المسئولية الجنائية لمقلد الموقع الالكترونى في مواجهة البنك:

٢٥٩- من خلال تدقيق النظر في نشاط المعتدين عند تقليد الموقع الإلكتروني للبنك على شبكة الإنترنت، نلاحظ أنهم لا يعمدون إلى إيجاد موقع إلكتروني مماثل ومطابق لموقع البنك في كل الصفات والخصائص، بل يقومون بتقليد العناصر التي تميز الموقع الإلكتروني، باعتبارها العناصر التي يعتمد عليها العملاء في التعامل مع موقع البنك، فيقومون بتقليد العلامة التجارية والعنوان الإلكتروني وصفحات الويب (Web) الخاصة بالبنك الإلكتروني بذات التصميم

وعدد الصفحات، على نحو ينخدع به عملاء البنك الإلكتروني فيقدمون على التعامل مع هذا الموقع المقلد على أنه الموقع الحقيقي للبنك الإلكتروني الذي يريدون التعامل معه.

ويعاقب قانون الملكية الفكرية المصري الصادر سنة ٢٠٠٢ في المادة (١/١١٣) على تزوير العلامة التجارية، حيث ينص على أن " يعاقب بالحبس مدة لا تقل عن شهرين وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه أو بإحدى هاتين العقوبتين كل من زور علامة تجارية تم تسجيلها طبقا للقانون أو قلدها بطريقة تدعو إلى تضليل الجمهور".

والواضح من صياغة النص أن المشرع المصري فرق بين التزوير والتقليد، على الرغم من أن التقليد طريقة من طرق التزوير. ويبدو أن المشرع قصد بهذه التفرقة توفير أقصى حماية ممكنة للعلامة التجارية ضد كافة أشكال ومظاهر الاعتداء عليها[١]، وإن كنا نرى اتساقا مع هذا المنهج ــ الساعي إلى تحقيق أقصى حماية ــ أن تستبدل كلمة الاصطناع في هذا النص بكلمة التزوير[٢].

أيضا نص قانون الملكية الفكرية الفرنسي في المادة ٣/٧١٣ [٣] على تجريم

(١) د. **شريف محمد غنام**، مسئولية البنك عن أخطاء الكمبيوتر في النقل الإلكتروني للنقود، مرجع سابق، ص ١١٩.

(٢) **التقليد** بمفهومه العام يعنى المحاكاة، أي صناعة شيء على غرار شيء آخر موجود. ولا يشترط في التقليد المماثلة والمطابقة التامة، بل يكفى فقط مجرد المحاكاة على نحو ينخدع به الناس.
ويعرف **الاصطناع** بأنه إنشاء أو اختلاق شيء له مثال سابق، إلى حد يصل إلى المطابقة والمماثلة، على نحو يخدع الناس. انظر د. **السيد عتيق**، مرجع سابق، ص ١٢٧.

(٣) هذا القانون متاح على العنوان الإلكتروني التالي:

تقليد أو تزوير العلامة التجارية، وقد اشترط أن يقع التقليد أو التزوير من قبل شخص غير مالك للعلامة وبدون إذن مالكها.

وبناءً عليه يسأل المعتدى في مواجهة البنك الإلكتروني عن جريمة تزوير العلامة التجارية للبنك.

وكما سبق أن ذكرنا(١) يأخذ العنوان الإلكتروني (Domain Name) ذات حكم العلامة التجارية في هذا الصدد، حيث ينظر إليه على أنه أحد عناصر الملكية الصناعية، وذلك لتشابه وظيفة العنوان الإلكتروني مع عناصر الملكية الصناعية (كالعلامات والأسماء التجارية) في كونها وسيلة مميزة في مجال الدعاية والإعلان، وكذلك تطلب إجراءات خاصة للتسجيل للحماية، نضيف على ذلك ما يحيط وضع وتصميم العنوان الإلكتروني من عناصر الابتكار والجدة التي تتميز به عناصر الملكية الصناعية. وبناءً عليه يستفيد العنوان الإلكتروني من التنظيم القانوني المقرر لهذه العناصر، سواء بموجب نصوص تشريعية أو أحكام قضائية.

وفى جميع الحالات يجب على المحكمة أن تقضى (على سبيل العقوبات التبعية) بإغلاق الموقع المزيف، ومصادرة كافة الأجهزة والبرامج التي تم استخدامها في ارتكاب هذه الجريمة.

(ب) المسئولية المدنية لمقلد الموقع الالكترونى في مواجهة البنك:

٢٦٠- يستطيع البنك الإلكتروني الرجوع على المعتدين بالتعويض، إذا ثبت

---

http://www.droitenligne.com/matieres/prOpr-intell.html

(١) انظر سابقا، ص ١٥٩.

ارتكابهم لتقليد موقعه على شبكة الإنترنت، أو حتى فقط تقليد العلامة التجارية للبنك، على نحو يؤدى إلى إثارة اللبس والخلط في أذهان الأفراد، وذلك بعد إثبات البنك لذلك. ويعتمد البنك الإلكتروني في رجوعه على هؤلاء المعتدين على قواعد المسئولية التقصيرية (١٦٣ مدني مصرى)، والتي تقضى بأن "كل خطأ سبب ضررا للغير يلزم مرتكبه بالتعويض".

ويجب على المحكمة، عند تقدير مبلغ التعويض، أن تراعى مقدار الضرر الذي لحق بالبنك من جراء ذلك، سواء كان ضررًا ماديًا تمثل في خسارة مبالغ تم الحصول عليها نتيجة تقليد موقعه وخديعة عملائه، أو ضررًا أدبيًا نتيجة المساس بسمعة البنك وأمنه، على نحو قد يؤدى إلى عزوف الأفراد عن التعامل معه[١].

ولا يؤثر في استحقاق البنك للتعويض قيام المحكمة بإلزام المعتدين برد كافة المبالغ التي حصلوا عليها نتيجة تقليد موقع البنك.

ثانيا: مسئولية مقلد الموقع الإلكتروني للبنك في مواجهة العملاء:

٢٦١- **بالنظر** إلى نشاط المعتدى في مواجهة عملاء البنك، يلاحظ قيامه بخديعة هؤلاء العملاء للاستيلاء على أموالهم، بعد الحصول على البيانات الخاصة بالتعامل مع البنك الإلكتروني، وذلك من خلال استعمال موقع إلكتروني مشابه لموقع البنك. ولاشك في أن نشاط المعتدى على هذا النحو ينطوى على اعتداء على حقوق هؤلاء العملاء، مما يدفع للتساؤل عن مسئولية هؤلاء المعتدين في مواجهة عملاء البنك؟

---

(١) د. **محمد حسين منصور**، مرجع السابق، ص ٤٠٠.

ونعرض لذلك على النحو التالى :

(أ) المسئولية الجنائية لمقلد الموقع فى مواجهة العملاء:

٢٦٢- كما سبق أن ذكرنا[١]، لم يفرد المشرع المصري نصا خاصا باستعمال الوسائل الإلكترونية في ارتكاب جريمة النصب. لكن من خلال مطالعة نص المادة ٣٣٦ من قانون العقوبات المصريِ نلاحظ أنها تستوعب إمكانية وقوع جريمة النصب بالوسائل الإلكترونية، حيث جاء في عجز هذه المادة: "يعاقب بالحبس كل من توصلَ إلى الاستيلاء على نقود أو عروض أو سندات دين أو سندات مخالصة أو أي متاع منقول، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة....".

ومن خلال استعراض نشاط المعتدين قبل عملاء البنك الإلكتروني، نلاحظ قيامهم باستعمال وسائل احتيالية بهدف الحصول على أموال هؤلاء العملاء، مما يتحقق معه وفقا للقواعد العامة في قانون العقوبات جريمة النصب بركنيها المادى والمعنوي.

لكن من خلال مطالعة نظم قانونية آخري، تبين أنها تفرد نصا خاصا ينظم ارتكاب جريمة النصب باستخدام الوسائل الإلكترونية، مثل قانون العقوبات الياباني حيث نصت المادة (٢٤٦/٤) على أن يعاقب كل من استعان بمعلومات مبرمجة كاذبة أو أدخل هذا النوع من المعلومات في نظام كمبيوتر لشخص آخر

---

(١) انظر سابقا، ص ٤٢٤.

لحصول لنفسه أو للغير على ربح غير مشروع[1].

وبناءً عليه يمكن لأي عميل من عملاء البنك الإلكتروني في حالة خديعته وقيامه بالدخول على موقع البنك المقلد، والتعامل مع هذا الموقع على أنه موقع البنك، أن يرجع على المعتدين بالنصوص المنظمة لجريمة النصب.

(ب) المسئولية المدنية لمقلد الموقع فى مواجهة العملاء:

٢٦٣- أما فيما يتعلق بالمسؤولية المدنية للمعتدى، فأن عميل البنك الإلكتروني يملك الرجوع عليه بالتعويض عن كل ما أصابه من أضرار، على أن يشمل هذا التعويض ما لحقه من خسارة وما فاته من كسب نتيجة هذا النشاط وفقا للقواعد العامة في المسئولية التقصيرية.

كما يلتزم المعتدى في جميع الأحوال برد كافة أموال العميل التي تحصل عليها نتيجة ارتكابه لهذا النشاط.

لكن هل من المتصور أن تثور مسئولية البنك الإلكتروني في مواجهة العميل عن تقليد الموقع؟

٢٦٤- مسؤولية البنك عن تقليد موقعه الالكترونى في مواجهة العميل:

وفقا للقواعد العامة في المسئولية المدنية، سواء تلك الخاصة بالمسئولية العقدية أو التقصيرية في القانون المصري، لا مجال لرجوع العميل على البنك؛ حيث إن الأخير لم يصدر عنه أي خطأ يبرر قيام مسئوليته. ونضيف إلى ذلك أن

---

(١) د. شيماء عبد الغني محمد عطا الله، مرجع سابق، ص٧٥.

قواعد المسئولية المدنية الموضوعية، أو ما يعرف بتحمل التبعة[١] غير قـادرة أيضا على تمكين العميل من الرجوع على البنك الإلكتروني في حالة تقليد موقعه على شبكة الإنترنت، وذلك لما يلي:

أولا: أنه على الرغم من أن هذه المسئولية يغيب عنها ركـن الخطـأ كأسـاس للمسؤولية وتكتفي فقط بالضرر لانعقادها، إلا أن هذا لا يعنـى التخلـي التـام والمطلق عن فكرة الخطأ؛ حيث يجب أن يكون لنشاط المسئول دور غير مباشر في إحداث الضرر. فالتشريعات التي تأخذ بنظرية تحمل التبعة لا زالـت فكـرة الخطأ تلقى بظلالها على مفهوم المسئولية[٢].

ثانيا: أن القول بإمكانية قيام مسئولية البنك الإلكتروني في مواجهة عميلـه فـي حالة تقليد موقعه على شبكة الإنترنت وفقـا لقواعـد المـسئولية الموضـوعية (المجردة من فكرة الخطأ) قول فيه مبالغة شديدة لا تتوافق مع الاتجاهات الساعية إلى تشجيع إنشاء البنوك الإلكترونية العاملة عبر شبكة الإنترنـت، مـن أجـل ملاحقة ركب التطور في هذا الخصوص، الأمر الذي يحب معه مراعاة وجـود نوع من التوازن في مسؤوليات الأطراف المختلفة، خاصة في ظل مـا تـشهده شبكة الإنترنت من تطور كبير، يجعل من الصعب على البنك أن يضمن سلامة ومشروعية المواقع الإلكترونية الموجودة على شبكة الإنترنت.

لكن على الرغم من عدم التسليم بقيام مسؤولية البنك الإلكتروني في مواجهة

---

(١) وتتأسس هذه المسئولية على استبعاد فكرة الخطأ كأساس للمسئولية، والاكتفاء بركنين فقط لقيامها هما الضرر وعلاقة السببية. ونتيجة لذلك انتفاء الخطأ لا يعد سببا لـدفع هذه المسئولية.

(٢) د. **نورى حمد خاطر**، مرجع سابق، ص ١٨١٨.

عميله على أساس نظرية تحمل التبعة في حالة تقليد موقعه. إلا أنه يبدو لنا إمكانية قيام هذه المسئولية في حالة واحدة، وهي حالة أن وصل إلى علم البنك وجود تقليد لموقعه على شبكة الإنترنت ولم يقم على الرغم من ذلك باتخاذ الإجراءات اللازمة لوقف هذا الاعتداء، أو تخاذل في اتخاذها، حيث يعد هذا تقصيرا من جانب البنك يمكن معه للعميل الرجوع عليه بقواعد المسئولية العقدية، وذلك لأن البنك يلتزم في كافة تعاقداته مع عميله بأن يتخذ كافة الإجراءات اللازمة لتأمين التعاملات المصرفية عبر شبكة الإنترنت، والتي من بينها التصدي لمحاولات تقليد موقعه الإلكتروني. ويسأل البنك في ذلك، سواء ورد النص على هذا الالتزام صراحة في العقد الذي يحكم علاقته بالعميل أم لم يرد، وذلك باعتبار أن هذا الالتزام من مقتضيات العقد وفقا لطبيعة محله، والبيئة التي يتم فيها، كما تقضي المادة ١٤٨ من القانون المدني بذلك صراحة.

ويثور بمناسبة مسؤولية البنك في هذا الخصوص تساؤل يتعلق بالمعيار الذي يجب أن يقاس به التزام البنك في هذه الحالة.

من خلال مطالعة صيغ العقود (١) التي تتبناها البنوك بخصوص التزاماتها بتأمين معاملاتها المصرفية مع العميل عبر شبكة الإنترنت بصورة عامة، يتضح أن هذه البنوك تكتفي ببذل عناية وليس بتحقيق نتيجة.

---

(1) **Internet Banking Security**; available at:
http://www.eldersruralbank.com.au/internet-banking/internet-banking-security#internet_banking_security
Jyske bank, JBPB, Net Bank user agreement, (EN)-2007, available at:
http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf

ويبدو لنا عدم منطقية وعدالة هذا المعيار في قياس التزام البنك باتخاذ الإجراءات اللازمة لإيقاف الاعتداء على موقعه من خلال تقليده، خاصة في ظل علم البنك بوقوع هذا الاعتداء، الأمر الذي يتطلب إلزام البنك بتحقيق نتيجة في تأمين معاملات المصرفية مع العميل، ويأتي هذا التشديد في المسئولية في ظل أهمية وخطورة الاعتبارات الأمنية في نظام عمل البنك على شبكة الإنترنت، وذلك في ظل عالمية الشبكة وتفعمها بالمخاطر. وفي ضوء الطبيعة الخاصة للعمليات المصرفية وما تحتاج إليه من احتياطات أمنية مشددة، وعلىّ ذلك يجب على البنك أن يبادر باتخاذ كافة الإجراءات اللازمة لإيقاف الاعتداء من خلال الاتصال بالجهات المعنية لإيقاف عمل الموقع المقلد، كما يجب أن ينبه المتعاملين معه لوجود مثل هذا الموقع، وكيفية تجنب التعامل معه، كما يجب أن يتوجه للقضاء المختص لملاحقة المعتدين.

وترتيبًا على ذلك، لا يلتزم العميل في حالة أن أراد الرجوع على البنك بسبب إخلاله بهذا الالتزام أن يثبت خطأ البنك وتقصيره في اتخاذ الإجراءات اللازمة لمواجهة الاعتداء، حيث إن هذا الخطأ مفترض في جانب البنك بحكم طبيعة المسؤولية، ولا يملك البنك أن ينفى مسؤوليته في هذه الحالة إلا بإثبات السبب الأجنبي؛ كقوة قاهرة أو حادث فجائي.

ولم يظهر لنا من خلال مطالعة النظم القانونية المختلفة نص يعالج مسؤولية البنك في مواجهة العميل في حالة تقليد موقعه، الأمر الذي يعكس خضوع هذا الأمر للقواعد العامة سالفة الذكر.

المطلب الثاني

تعطيل نظام عمل البنك الإلكتروني على شبكة الإنترنت

Denial of service

٢٦٥- ظهر في الآونة الأخيرة شكل جديد من أشكال الهجمات التي تستهدف موقع البنك الإلكتروني على شبكة الإنترنت، وهو ما يطلق عليه تعطيل سير النظام (Denial of Service)[1]. وتسعى مثل هذه الهجمات إلى منع وحرمان عملاء البنك من الوصول إلى موقعه الإلكتروني على شبكة الإنترنت للحصول على الخدمات التي يقدمها[2].

والأمر على هذا النحو يستدعي إلى التعرض لتعريف تعطيل نظام عمل البنك كأحد صور الاعتداءات التي تستهدف أمنه، والوسائل التي يرتكب من خلالها هذا الاعتداء، والإجراءات الوقائية التي يجب أن يلتزم بها كل من البنك والعميل للحيلولة دون وقوع هذا الاعتداء، والمسؤولية القانونية عنها، وذلك على النحو التالي:

(١) ويعد الحرمان من الخدمة من أخطر صور الهجمات التي تتعرض لها المواقع الإلكترونية على شبكة الانترنت. وقد شهدت تزايد ملحوظا في السنوات الأخيرة. ومن أهم المواقع التي تعرضت لمثل هذه الهجمات موقع (CNN)، وموقع (YAHOO) وموقع (eBay)، واكتشف أن هذه الخدمات قد صدرت عن أفراد خارج الولايات المتحدة الأمريكية.

David Jefferson and others, Analysis of the electronic registration and voting experiment (serve), Security analysis of serve, January, 2004, p 18

(2) **Internet security: Distributed denial of service attacks, OCC alert**, available at: www.ffiec.gov/ffiecinfobase/resources/infosec/occ-al_2000_01_net_sec_denial_serv_attack.pdf

Katyal, Neal Kumar; Op. Cit, p. 44.

التالي:

١- تعريف تعطيل نظام عمل البنك:

٢٦٦- يعرف تعطيل النظام الإلكتروني[١] بأنه "نوع من الهجمات الإلكترونية المصحوبة بنوايا خبيثة، تهدف إلى إغراق (overflow) أو تعطيل (jam) الموقع الإلكتروني بكثرة الطلبات، على نحو يتسبب في إغلاق الموقع، وحرمان العملاء من الحصول على الخدمة التي يقدمها هذا الموقع.

وعرف[٢] أيضا بأنه عبارة عن منع أو تعطيل التواصل بين طرفين عن طريق إحداث تكدس وازدحام في خطوط الاتصال فيما بينهم.

٢- طرق تعطيل نظام عمل البنك على شبكة الإنترنت:

٢٦٧- تبدو أهمية التعرض للطرق المتبعة من قبل المعتدين في الإخلال بسير نظام البنك، من أجل التعرف على طبيعة النشاط الذي يقومون به، لتحديد طبيعة المسؤولية القانونية الناشئة عن هذا النشاط، ولتنبيه البنك لهذه الطرق، من أجل تحميله المسؤولية القانونية في اتخاذ الاحتياطات اللازمة لمواجهة هذا النشاط.

وتتعدد الطرق التي يسلكها المعتدون للوصول إلى منع عملاء البنك الإلكتروني من الحصول على خدمات البنك، وهي مثل[٣]:

---

(1) **Thomas C. Glaessner, Tom Kellermann, Valerie McNevin**; Op, Cit, p. 160.

(2) **Mukesh M. Prabhu, S.V. Raghavan,** Security in computer networks and distributed systems, Computer Communications, 1996 (379-388), p. 380.

(3) **Katyal, Neal Kumar**; **Op**. Cit, p. 44.

- إحداث إشغال للموقع الإلكتروني للبنك على نحو يتسبب في منع الوصول إليه عبر شبكة الإنترنت، وذلك كمحاولة إرسال كم هائل من رسائل البريد الإلكتروني إلى موقع البنك تكون أكبر من قدرة البنك على الاستيعاب، على نحو يسبب إغراق وتعجيز الموقع عن التعامل(١).

- منع الاتصال بين نقاط العمل على الموقع على نحو يمنع الحصول على ما تقدمه هذه النقاط من خدمات، وذلك مثل حذف روابط الاتصال (Links) التي تربط الصفحة الرئيسة (Home page) للبنك بالصفحات الفرعية الخاصة بالخدمات المصرفية التي يقدمها البنك.

- منع وصول الخدمة المصرفية لمؤسسة معينة أو لفرد معين(٢) وذلك من خلال قطع سبل الاتصال التي تربط بين البنك وإحدى المؤسسات التي تحصل على خدمة معينة من البنك، كأحد المتاجر التي ترتبط بموقع البنك، والتي تقبل الدفع ببطاقات الائتمان التي يصدرها البنك الإلكتروني.

---

(١) **د. حسين الماحي**، نظرات قانونية في التجارة الإلكترونية، مرجع سابق، ص٢٩٠.

(٢) وقد تمارس بعض الجهات الإعلانية حملات الإغراق بقصد مشروع وهو توزيع أكبر قدر من الإعلانات على أصحاب البريد الإلكتروني بهدف الإعلان عن المنتجات محل هذه الإعلانات، فيتسبب ذلك في إحداث إغراق لصناديق البريد الإلكتروني على النحو الذي يصعّب على أصحابها استعمالها. لذلك صدرت عن البرلمان الأوربي توجيهات تفيد تمكين مستخدمي البريد الإلكتروني من تسجيل اعتراضهم على مثل هذه الرسائل، كما تضمنت مبادرة لندن للتبادل عبر الانترنت إصدار بيان يحتوى على الممارسات الجيدة التي يجب أن تتبع في هذا الخصوص، وكان من بينها ما يفيد حظر الإغراق بالإعلان.

Kit Burden; Op. Cit, p. 249; **Denial of Service Attacks,** Coordination center, available at: http://www.cert.org/tech_tips/denial_of_service.html

• إرسال فيروسات خاصة لتعطيل خادم التطبيقات المصرفية الملحق بـــالموقع الإلكتروني للبنك، وذلك على النحو الذي يعطل هذا الخادم عن القيام بوظيفته لاستقبال طلبات عملاء البنك(1).

ويعتمد المعتدون في ارتكاب مثل هذا النوع من الهجمات على بعض الثغرات الفنية والأمنية، والتي تدعو الحاجة لذكرها، باعتبارها التزامـــات يجـــب عليـــه الالتزام بها في مواجهة العميل بسد هذه الثغرات لتـــأمين معاملاتـــه، وتحمـــل المسؤولية القانونية عن التقصير في ذلك في مواجهة العميل. ومـــن أهـــم هـــذه الثغرات:

- احتواء شبكة البنك الإلكتروني على مصادر محدودة وقابلة للنفاذ:

كما سبق أن ذكرنا تقوم رفض الخدمة كإحدى الهجمات التي تستهدف أمـــن البنك على الحيلولة دون وصول العميل وتعامله مع موقع البنك. ويجد المعتـــدى

---

(1) **David Jefferson and others**; Op, Cit, p. 18;

د.**حسين الماحى**، نظرات قانونية في التجارة الإلكترونية، مرجع سابق، ص ٢٩١.

- ويعتقد العديد من الخبراء بشأن أمن الشبكات أن مثل هذه الهجمات تتم من خـــلال قيام المعتدين بالاستيلاء على مواقع إلكترونية على شبكة الانترنت (شركات، أجهزة حكومية، جامعات) واستغلالها بغير علم من أصحابها لمهاجمة المواقـــع الأخـــرى المستهدفة بإعاقة النظام (موقع البنك الإلكتروني)، الأمر الذي يفرض على جميـــع المواقع العاملة على شبكة الانترنت أن تتواجد في حالة يقظة دائمة، وكشف دوري مستمر لنشاط موقعهم على الشبكة، ومحاولة إبلاغ الجهات المختصة فـــي حالـــة وجود أي صورة من صور الاستغلال غير المشروع على مواقعهم.

Internet Security: Distributed Denial of Service Attacks, OCC alert, Op, Cit, available www.ffiec.gov/ffiecinfobase/resources/info_sec/**occ**-at:al_2000_01_net_sec_**denial**_serv_attack.pdf

سبيله للوصول إلى ذلك باستنفاذ أو تعطيل الأجهزة العاملة على شبكة البنك؛ فسعة الاستقبال والتخزين لأجهزة البنك محدودة وقابلة للنفاد، فيلجأ المعتدى إلى غمرها برسائل وطلبات وهمية، على النحو الذي يعطلها عن العمل(١).

- **ارتباط أمن موقع البنك بأمن شبكة الإنترنت:**

اتصال شبكة البنك الداخلية بشبكة عالمية مترامية الأطراف كشبكة الإنترنت يجعل تأمين البنك مرتبطاً نوعا ما بأمن الشبكة بصورة عامة. فوجود موقع تخريبي على الشبكة من شأنه أن يهدد بإخلال سير نظام البنك بسهولة من خلال الاتصال عبر شبكة الإنترنت، الأمر الذي يفرض على البنك ضرورة إجراء عمليات مسح دورية تستهدف التنقيب عن هذه المواقع، والإبلاغ عنها، وتنبيه عملائه إليها، واتخاذ كافة الاحتياطات الأمنية الكفيلة بمنع أية هجمات ترد من هذا الموقع(٢).

٣- الإجراءات الوقائية ضد الدخول غير المشروع:

٣٦٨- لاشك أن الإخلال بالنظام كأحد الأنشطة التي تستهدف أمن البنك الإلكتروني تشكل تهديدا كبيرا لقدرة البنك على العمل على شبكة الإنترنت، الأمر الذي يحتاج من البنك إلى أن يتوخى الحذر الشديد للحيلولة دون وقوع مثل هذا الأمر. هذا الحذر يتأتى من خلال مجموعة من الإجراءات الوقائية التي يجب أن يتحصن بها البنك، والتي تعد بمثابة التزامات قانونية، يخضع البنك في مدى

---

(1) **Denial of Service Attacks,** Coordination center. available at: http://www.cert.org/tech_tips/denial_of_service.html

(2) **Kevin J.Houle, George M. Weaver**. Trends in denial of service attack technology. coordination center. v1.0. October 2001, p. 2.

الالتزام بها لإشراف جهة الرقابة. كما أن الإخلال بهذه الإجراءات من قبل البنك تجعله في مركز المقصر تجاه العميل، ومن ثم يتحمل المسؤولية عن تعويض الأضرار التي تلحقه نتيجة لذلك. ومن أهم الإجراءات التي يجب على البنك اتخاذها ما يلي[1]:

أ- يجب على البنك الإلكتروني أن يتفادى وجود أجهزة أو برامج أو وصلات معطلة في شبكة البنك، وذلك حتى لا تكون بمثابة نقاط ضعف يستغلها المعتدى في تنفيذ هجمات الإخلال بالنظام، من خلال توجيه مسار الطلبات القادمة من العملاء إلى المناطق المعطلة، ومن ثم يجب على البنك أن ينظم عمليات فحص وصيانة بصورة دورية ومنتظمة لجميع مكونات شبكة البنك، حتى يتفادى وجود أجهزة معطلة.

ب-يجب على البنك الإلكتروني أن يوزع مهام عمل الموقع على جميع الأجهزة المرتبطة بالشبكة، وأن يستعين بأجهزة بديلة لاستخدامها في حالات الطوارئ، على نحو يجعل هناك نوعا من الوفرة والاستمرارية في العمل.

ج-يجب على البنك الإلكتروني أن يراقب أداء العمل على الموقع باستمرار، من خلال الاستعانة بأجهزة إنذار وتنبيه بحيث تعطى إشارات في حالة وجود ضغط عمل على الموقع بشكل غريب، أو وجود تلاعب بأحد مكونات الموقع على شبكة الإنترنت، وأيضا من خلال فحص دوري ومنتظم لمستوى الأداء، وإنشاء معايير معينة لقياس مستوى هذا الأداء وكتابة تقارير مفصلة عن

(1) **Adrian McCullagh -William Caelli**; Op. Cit. p. 353.

ذلك[1].

د- يجب على البنك الإلكتروني أن يتبنى خطة طوارئ، بحيث تتضمن هذه الخطة كيفية إدارة موقع البنك في حالة وقوع أي عطل في الأجهزة، وكذلك الطرق البديلة التي يمكن اللجوء إليها لضمان نوع من الاستمرارية في الأداء. يضاف إلى هذا أن البنك عادة ما يحتفظ بحقه في تعليق أو تحديد أو إيقاف تقديم الخدمة المصرفية عبر شبكة الإنترنت إذا ما واجه ظروفًا تستدعى هذا، وذلك بالنص صراحة في العقد الذي يحكم علاقته بالعميل على تمتعه بهذا الحق في مواجهة العميل. لكن يجب علي البنك أن يخبر بالعميل قبل هذا الإجراء بمدة حتى يستعد لذلك[2].

٤- المسؤلية القانونية لمعطل نظام البنك الإلكتروني:

٢٦٩- رأينا كيف أن الإخلال بالنظام كأحد الأنشطة التي تستهدف أمن البنك الإلكتروني ذو تأثيرًا كبير على نشاط البنك العامل عبر شبكة الإنترنت، وأن هذا التأثير يظهر في الحيلولة بين البنك والعميل على نحو يؤدى إلى تعطيل البنك عن تقديم الخدمات المصرفية، الأمر الذي يدعونا للتعرف على مسئولية المعتدى

---

(1) **Denial of Service Attacks,** Coordination center, available at: http://www.cert.org/ tech_tips/ denial_of_service.html

(2) (The Bank may, where considered appropriate for your or the Bank's protection, suspend, withdraw or restrict the use of JBPB Netbank Service or any part thereof. You will be informed as soon as practicable if such action is taken). **JYSKE BANK**, JBPB, Net Bank user agreement, (EN)-2007, available at: http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf

تجاه كل من البنك الإلكتروني والعميل على النحو التالي:

أولا: مسئولية معطل النظام في مواجهة البنك الإلكتروني:

٢٧٠- بالنظر لطبيعة نشاط المعتدى تجاه البنك في الفرض السابق، يمكن القول بأن مسؤوليته عن هذا النشاط تنظم على النحو التالي:

ا- المسئولية الجنائية لمعطل النظام فى مواجهة البنك:

٢٧١- في الواقع يخلو قانون العقوبات المصري من نص خاص ينظم الإخلال بالنظام كنشاط إجرامي، بل حتى الصور التقليدية للجرائم المعروفة في هذا القانون. غير قادرة على أن تستوعب هذا النشاط.

أما عن الوضع في الأنظمة القانونية الأخرى فهو مختلف، حيث تضمنت المادة ٣٢٣-٢ من قانون العقوبات الفرنسي ما يفيد تجريم هذا النشاط حيث نصت على أن " يعاقب على الإعاقة أو الإخلال بسير نظام معالجة المعلومات بالحبس مدة لا تزيد على خمس سنوات والغرامة التي لا تزيد على ٣٠٠ ألف يورو".

أيضا القانون الإنجليزي سن قانونا خاصا بإساءة استعمال الكمبيوتر Computer Misuse Act صدر عام ١٩٩٠[(١)] تضمن نصا قريبا من النص السابق حيث جرم " كل تعديل لمحتوى الكمبيوتر دون إذن صاحب الحق فيه".

وقد قضى القضاء الفرنسي تطبيقا لذلك "بوقوع الجريمة من المتهمين الذين

---

(١) هذا القانون متاح على الموقع الإلكتروني التالي:
http://www.publications.parliament.uk/pa/cm200405/cmbills/102/2005102.htm

دأبوا على إرسال رسائل كثيرة بنية الغش عبر نظام كمبيوتر، مما أدى إلى إرباك النظام المتلقي لهذه الرسائل، والتي تمثلت في طلبات اشتراك في مسابقة من المسابقات التي يمكن أن تنتهي بالحصول على جوائز"[1].

وفي حكم آخر للقضاء الفرنسي ذهب للحكم إلى توافر جريمة الإخلال بالنظام من المتهم الذي قام بإرسال رسائل كثيرة إلى أحد الأجهزة الخاصة بإحدى الشركات المنافسة، موهما هذا الجهاز أن الرسائل تصل إليه من أجهزة متعددة، وتتضمن طلبات شراء من الشركة، وقد كانت تلك الطلبات غير جدية، وكان هدف المتهم منها أن يشغل الأجهزة الخاصة بهذه الشركة حتى تكون عاجزة عن تلقى طلبات جديدة، ويضر بها في النهاية"[2].

وبناء عليه يسأل المعتدى جنائيا في مواجهة البنك الإلكتروني، وذلك في حالة قيامه بارتكاب أي نشاط من شأنه أن يخل بنظام عمل البنك على شبكة الإنترنت، وذلك وفقا للقانون الفرنسي، وأن كنا نهيب بالمشرع المصري بضرورة التصدى لمثل هذا الفعل الذي من شأنه تهديد وجود وعمل البنك على شبكة الإنترنت، وذلك بنص خاص، حتى يغلق الباب أمام اللجوء إلى القياس المحظور في المجال الجنائى.

والتساؤل الذي يطل علينا في هذا الخصوص، يتعلق بمدى مسؤولية مزودي الخدمة إذا ما قام أحدهم بارتكاب أي نشاط من شأنه أن يخل بنظام عمل البنك

---

(1) **Paris**, Flash, n 18, 5 avr.1994; Available at: http://encyclo.erid.net/document.php?id=198

(2) **CA Paris**., Juris-Data, n 020128, 14 janv.1997; Available at: http://www.juriscom.net/uni/mem/06/crim01.htm#nbp72

على شبكة الإنترنت بقصد الإضرار بالبنك.

من المتصور، بالنظر للدور الكبير الذي يضطلع به مزودو الخدمة في نظام عمل البنك على شبكة الإنترنت، إمكانية وقوع جريمة الإخلال بالنظام من قبلهم، وذلك بحكم قربهم الشديد من أجهزة البنك. ونظام عمله، حيث يمكن لهم استغلال ذلك في إعاقة نظام عمل البنك بأي صورة. ومن ثم في حالة وقوع هذه الفعل من أحدهم يسرى في حقهم ما سبق ذكره في حالة ارتكاب هذا الفعل من أي مهاجم.

لكن هل يمكن القول بوقوع هذه الجريمة في حالة إخلال مزودي الخدمة بتنفيذ عقود صيانة الأجهزة أو توريد قطع غيار لها على نحو يتسبب في عدم قدرة العملاء على التعامل مع البنك؟

ذهب اتجاه[(١)] للقول، بأن حدوث إخلال بعقد من عقود الصيانة أو توريد الأجهزة اللازمة لعمل البنك وتعامله مع العملاء من قبل مزودي الخدمة، على نحو يتسبب في تعطيل نظام العمل مع البنك لا يعتبر من قبيل النشاط المعاقب عليه

لكننا لا نتفق مع هذا الرأى، ونرى أننا في هذا الفرض يجب أن نفرق بين حالتين:

الحالة الأولى: هي إذا كان إخلال مزودي الخدمة بالتزاماتهم ليس بدافع الإضرار بالبنك وعملائه، ولكن لظروف قاهرة أدت إلى عدم قدرتهم على تنفيذ التزاماتهم تجاه البنك، على النحو الذي تسبب في تعطيل أجهزة البنك؛ حيث في

---

(١) **د. شيماء عبد الغنى محمد عطا الله**، مرجع السابق، ص ١٥٠.

هذه الحالة لا يمكن القول بوقوع جريمة إعاقة النظام، وذلك لعدم توافر القصد الجنائي.

الحالة الثانية: وهي حالة ما إذا كان هناك دافع للغش أو الإضرار لدى مزودى الخدمة في امتناعهم عن تنفيذ التزاماتهم مع البنك، هنا نرى أن الجريمة تقع، وذلك بتحقق ركنيها المادي (عدم تنفيذ الالتزام المكلف به) والمعنوي (قصد الإضرار)، ويمكن إثبات توافر القصد الجنائي في هذه الحالة، بإثبات عدم توافر أسباب جدية تقف وراء امتناع مزودي الخدمة عن تنفيذ التزاماتهم، ولكن فقط الإضرار بالبنك وعملائه.

ب- المسئولية المدنية لمعطل النظام فى مواجهة البنك :

٢٧٢- في حالة ثبوت ارتكاب المعتدى لنشاط الإخلال بالنظام في حق البنك الإلكتروني، فأن الأخير يملك الرجوع على الأول بالتعويض المناسب، وذلك بموجب قواعد المسئولية التقصيرية؛ حيث باشر المعتدى نشاطًا غير مشروع سبب ضرر للبنك (المادة ١٦٣ مدني مصري).

ويسأل المعتدى عن كل ضرر لحق بالبنك، سواء كان هذا الضرر ماديا تمثل في تلف أجهزة أو برامج البنك، أو ضرر معنوى تمثل في الإساءة لسمعة البنك، وزعزعة الثقة في خدماته أمام العملاء.

ويثور التساؤل حول مدى مسؤولية مقدم الخدمة في مواجهة البنك في حالة قيامه بهذا النشاط؟

وفي حالة وقوع خلل في نظام عمل البنك بسبب أحد مقدمي الخدمة نتيجة الاخلال بالتزامه التعاقدي تجاه البنك- سواء كان ذلك بحسن أم بسوء نية؛ فإن

البنك يملك الرجوع عليه بالتعويض بموجب قواعد المسؤولية العقدية. ويكفي البنك الإلكتروني في هذا الفرض أن يثبت عدم تحقق النتيجة المرجوة من التعاقد حتى تقوم مسئولية مقدم الخدمة، دون أن يكلف بإثبات خطئه، الذي يعد مفترضًا في هذه الحالة، ولا يستطيع الأخير دفعها إلا بإثبات السبب الأجنبي، وذلك بالنظر إلى أن التزام مقدم الخدمة بصيانة الأجهزة وتشغيلها هو التزام بتحقيق نتيجة.

ثانيا: مسئولية معطل النظام في مواجهة العملاء:

(أ) المسئولية الجنائية لمعطل النظام فى مواجهة العملاء:

٢٧٣- ليس من المتصور أن تثور المسئولية الجنائية لمعطل النظام في مواجهة عميل البنك الإلكتروني عن نشاط الإخلال بالنظام، وذلك في حالة الاعتداء المباشر من قبل المعطل على موقع البنك الإلكتروني، حيث إن هذا النشاط لا يشكل اعتداءً مباشرا على عميل البنك. لكن في حالة وقوع نشاط الإخلال بالنظام نتيجة اعتداء المعتدى على أجهزة أو وسائل الاتصال الخاصة بالعميل، فإن المسئولية الجنائية للمعتدى في هذه الحالة تقوم وفقا لما سبق ذكره بخصوص المسئولية الجنائية للمعتدى قبل البنك الإلكتروني[١].

(ب) المسئولية المدنية لمعطل النظام فى مواجهة العملاء:

٢٧٤- يشكل نشاط تعطيل النظام في كافة الأحوال (أي سواء كان الاعتداء على أجهزة البنك أو أجهزة العميل) عملا غير مشروع في نظر القانون المدني؛ وذلك نظرا لاتساع نطاق المسؤولية المدنية (التقصيرية) عن المسئولية الجنائية، حيث

(١) انظر سابقا، ص ٥٤٧.

تقضى الأولى بأن كل خطأ سبب ضررا للغير يلزم مرتكبه بالتعويض[1].

وبناء عليه يملك عميل البنك الإلكتروني الرجوع على المعتدى لتعويض الأضرار التي تلحق به من جراء ارتكاب الأخير لنشاط الإخلال بالنظام. ويجب على المحكمة عند تقدير التعويض أن تراعى ما لحق العميل من أضرار (سواء ما لحقه من خسارة أو ما فاته من كسب) تسببت فيه نشاط المعتدى.

أما في حالة وقوع هذا النشاط من قبل أحد العاملين لدى البنك، فأن العميل يملك الرجوع عليه بالتعويض وفقا للقواعد السابقة بخصوص المسئولية المدنية للمهاجم. فضلاً عن إمكانية رجوع العميل على البنك الإلكتروني بموجب قواعد مسئولية المتبوع عن أعمال تابعيه، والتي تقضى بالمسئولية المدنية للمتبوع (البنك الإلكتروني) عن أعمال تابعيه (العاملين لدى البنك) في حالة وقوع خطأ منهم أثناء عملهم لدى المتبوع أو بسبب هذا العمل[2]. وفى هذه الحالة تنعقد المسئولية المدنية للبنك في مواجهة العميل، والذي يستطيع الرجوع على العامل مباشرة أو الرجوع على البنك والعامل معا على سبيل التضامن، ولن يستطيع البنك دفع هذه المسئولية بإثبات انتفاء الخطأ من جانبه[3].

أما في حالة وقوع هذا الفعل نتيجة إخلال أحد مقدمي الخدمة بالعقد الذي يربط بينه وبين البنك الإلكتروني، فإن العميل لا يملك الرجوع على مقدم الخدمة بموجب قواعد المسئولية العقدية، حيث لا توجد رابطة عقدية بينهما. كذلك لا

---

(١) م ١٦٣ القانون المدنى المصرى.

(٢) حيث تنص المادة ١٧٤ من القانون المدنى المصري على "يكون المتبوع مسئولا عن الضرر الذى يحدثه تابعه بعمله غير المشروع، متى كان واقعا منه في حالة تأدية وظيفته أو بسببها".

(٣) د. أحمد شوقى عبد الرحمن، مرجع السابق، ص٣٢٧.

يملك الرجوع على البنك بموجب مسئولية التابع عن أعمال تابعيه، حيث إن العقد المبرم بين البنك الإلكتروني ومقدم الخدمة ليس عقد عمل، بل يتم تكييف هذه العقود في الغالب على أنها عقود مقاولة[1] (حيث لا يملك رب العمل فيها سلطة فعلية على المقاول في أداء عمله)، ومن ثم لا يعد مقدم الخدمة تابعًا للبنك. .

لكن يمكن القول بأن العميل في حالة وقوع نشاط الإخلال بالنظام، (نتيجة إخلال أحد مزودى الخدمة بالعقد المبرم بينه وبين البنك الإلكتروني) يملك الرجوع على البنك بموجب قواعد المسئولية الموضوعية (تحمل التبعة)، فالبنك لم يصدر عنه خطأ في هذه الحالة، لكن الضرر الذي لحق العميل تسبب فيه نشاط البنك – بصورة غير مباشرة – نتيجة إخلال أحد مقدمي الخدمة بالعقد المبرم بينهما. وبعد أن يرجع العميل على البنك الإلكتروني، يملك الأخير الرجوع على مقدم الخدمة بموجب العقد المبرم بينهما.

المطلب الثالث

الدخول غير المشروع لنظم البنك الإلكتروني على شبكة الإنترنت

(Unauthorized Access)

٢٧٥- يقتضى الحديث عن الدخول غير المشروع كأحد أخطر صور الاعتداءات التى تستهدف أمن البنك تحديد المقصود بالدخول غير المشروع، وصور الدخول غير المشروع لموقع البنك، والطرق التى يسلكها المعتدون لذلك،

---

(١) د. **محمد حسين منصور**. مرجع السابق، ص٤٠.

والاجراءات الوقائية للحيلولة دون وقوعه، ومسؤلية مقتحم نظـام البنـك عـن الدخول غير المشروع، وذلك على النحو التالى:

١- تعريف الدخول غير المشروع لنظم البنك الإلكترونى:

٢٧٦- يعد اقتحام النظام الإلكتروني للبنك من خلال الدخول غير المشروع إلى النظام الداخلي الخاص بالبنك من أخطر صور الانتهاكات التي يمكن أن يتعرض لها البنك(١). وتعلل هذه الخطورة؛ بأن الدخول غير المشروع للبنك هو بمثابـة حلقة أولى في سلسلة من الانتهاكات(٢). فقد يقوم المعتدى بعد الدخول بالمـساس بسرية البيانات الموجودة لدى البنك، وذلك من خلال الاطلاع عليها، وقد يقـوم بالمساس بسلامة هذه البيانات من خلال تعديلها أو محوها، وقد يقـوم بزراعـة الفيروسات لتدمير الملفات المخزنة، وقد يقوم باستخدام أنظمة البنك الإلكترونـي كأداة لارتكاب الجرائم (كما لو قام بإجراء تحويلات غير مـشروعة، أو سـرقة أرقام بطاقات الائتمان(٣)، أو نشر مواد غير قانونية على موقع البنك)(٤)، بل قـد

(١) **د. محمد عبد الرحيم سلطان العلماء**، جرائم الانترنت والاحتـساب عليهـا، مـؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون (جامعـة الإمـارات العربيـة المتحدة)، ٢٠٠٠، ص٨.

Michael P. Dierks; Op, Cit, p. 310.

(٢) **د.عبد الله حسين محمود**، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهـضة العربية، الطبعة الأولى، ٢٠٠١، ص٩٥.

(٣) **د. حسين الماحى**، نظرات قانونية في التجارة الإلكترونية، مرجع سابق، ص ٢٩٠.

Zakaria I.Saleh; Op, Cit, p. 9; **Graham Smith**; Op. Cit, p. 278.

(٤) **يونس عرب**، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢، المركز العربي للدراسات والبحوث الجنائية - أبو ظبي ١٠-١٢ /٢/٢٠٠٢، ص١٦. متاح على العنوان التالي:

http://www.arablaw.org/Download/CyberCrimes_General.doc

يسعى المعتدى إلى إفقاد القائمين على إدارة البنك السيطرة عليه، وذلك كما لو تمكن بعد الدخول إلى نظام البنك الداخلي من تغير كلمة المرور، حيث لن يستطيع أحد الدخول على نظام البنك غيره، دون القائمين على إدارة البنك. أيضا يمكن للمهاجم أن يعمل على الإخلال بنظام عمل البنك، وذلك من خلال تحميل برامج من شأنها أن تؤدى إلى تنفيذ تعليمات غير مطلوبة، أو برامج تعمل على الإبطاء من سرعة العمل على الموقع. كذلك يمكن للمهاجم أن يقوم بزرع أجهزة للتجسس داخل شبكة البنك الإلكتروني بحيث يستطيع من خلال هذه الأجهزة نقل كل المعلومات التي تدخل أو تخرج من البنك[١].

وعلى ذلك يمكن القول إن أكثر حالات الانتهاكات التي تحدث للبنك الإلكتروني تبدأ بالدخول غير المشروع لنظام البنك العامل على شبكة الإنترنت[٢].

وقد عرف الدخول غير المشروع للبنك الإلكتروني، بأنه عبارة عن اقتحام النظم الداخلية للبنك، والمصحوب بنيات خبيثة تهدف إلى التعدى على أمنه[٣].

(١) د. **شيماء عبد الغنى محمد عطا الله**، مرجع السابق؛ ص١١٤

(٢) وفى عام ٢٠٠٣، ووفقا لإحصائية الأنشطة غير المشروعة الخاصة بانتهاكات الدخول غير المشروع التي تقع على أجهزة الكمبيوتر المتصلة بشبكة الانترنت أظهرت أن هناك ٣,٢٢٩ حالة انتهاك حدثت وتسببت في خسارة، قدرت ٢,٢ بلايين دولار، انظر:

Thomas C. Glaessner, Tom Kellermann, Valerie McNevin; Op, Cit, p. 87.

(3) Computer hacking and unauthorized access laws, Article available at :
http://www.ncsl.org/programs/lis/CIP/hacklaw.htm

٢- صور اقتحام الموقع الإلكتروني للبنك:

٢٧٧- تبدو أهمية التعرض لأنواع الدخول غير المشروع لأنظمة البنك الإلكتروني في التعرف على طبيعة النشاط الذي يقوم به المعتدى تجاه البنك، من أجل وضع توصيف قانوني مناسب لهذا النشاط، وكذلك لتنبيه البنك إلى حالات وطرق الدخول غير المشروع، وذلك لممارسة لاتخاذ الاحتياطات القانونية والأمنية للتصدي لمثل هذه الهجمات، ويمكن أن يظهر الدخول غير المشروع للبنك الإلكتروني في أحد فرضين[1]:

الأول: الدخول من قبل أحد العاملين لدى البنك، ويتمثل في قيام أحد العاملين لدى البنك بالدخول على أحد الأجهزة الخاصة بالبنك وهو غير مختص، أو غير مصرح له بالدخول على هذا الجهاز، أو مصرح له بالدخول ولكنه تجاوز الحدود المسموح له بالدخول عليها.

الثاني: ويتمثل في قيام أحد الأشخاص من الخارج (من غير العاملين) بالدخول على أجهزة البنك، ويمكن أن يحدث هذا الفرض في حالتين:

أ- وهي حالة الدخول على أجهزة البنك في أماكن تواجدها، والاطلاع على ما بها من ملفات.

ب- وهي حالة الدخول على أجهزة البنك عن بعد، وذلك من خلال الاتصال بشبكة الإنترنت.

ويعد الفرض الأخير من المخاطر المستجدة في نظام عمل البنوك العاملة عبر

---

(1) Michael P. Dierks, Op. Cit, p. 324.

شبكة الانترنت. وتظهر خطورة هذا الفرض في ارتباط الشبكة الداخلية للبنك بشبكة الانترنت المفتوحة على العالم بأسره، حيث تشكل نقطة ضعف يعمل المعتدون على استغلالها لتنفيذ هجمات الدخول غير المشروع لأجهزة البنك الإلكتروني[١]. فعلى الرغم من وجود بعض أشكال التعاون فيما بين البنوك في صورة اتحادات لتنفيذ بعض العمليات المصرفية فيما بينها (كالتحويل الإلكتروني للنقود)، وذلك من خلال اتصال هذه البنوك فيما بينها بشبكات داخلية، إلا أنها لم تكن معرضة للدخول غير المشروع على أنظمة أحد البنوك الداخلة في هذا الاتحاد؛ حيث إنها شبكات مغلقة، الدخول إليها مقصور على الأعضاء فيها فقط[٢]. لكن الوضع بالنسبة للبنوك العاملة عبر شبكة الإنترنت مختلف، وذلك بسبب اتصال شبكة البنك الإلكتروني بشبكة الإنترنت، ومن ثم فهذا الأمر يشكل خطورة كبيرة على البنك الإلكتروني ما لم يكن محاطا بسياج أمنى قوى[٣].

٣- طرق اقتحام موقع البنك الإلكتروني:

٢٧٨- تتعدد الطرق التي يلجأ إليها المعتدون لاقتحام الموقع الإلكتروني للبنك، وذلك على النحو التالي:

---

(1) **Thomas C. Glaessner, Tom Kellermann**; Op, Cit, p. 1.

(٢) ومن أشهر هذه الاتحادات جمعية سويفت في الولايات المتحدة الأمريكية (SWIFT) والتي كانت تربط بين البنوك وبعض المؤسسات المالية للتعاون فيما بينهما في تنفيذ بعض العمليات المصرفية كالتحويل الإلكتروني للأموال. انظر:

Thomas C. Glaessner, Tom Kellermann, Valerie McNevin; Op, Cit, p. 88; **G C Chalikias,** Op, Cit, p. 1.

(3) **Graham Smith;** Op. Cit, p. 277.

أ- تصديع كلمة المرور (Password Cracking):

يقصد بتصديع كلمة المرور، تخمين أو استنتاج كلمة المرور الخاصة بالتعامل مع البنك الإلكتروني العامل عبر شبكة الإنترنت، وذلك من أجل الدخول إلى أجهزة الكمبيوتر أو الشبكة الخاصة بالبنك(١).

وتتلخص عملية تصديع كلمة المرور، في محاولة محاكاة الخوارزميات التي تستخدم في تشفير كلمات المرور، باستخدام برامج أعدت خصيصا لهذا الغرض، حيث تعمل على إنتاج شفرات مستحدثة تناظر الشفرات المستخدمة في تكوين كلمة المرور الأصلية(٢).

ويعد من أكثر الطرق للدخول غير المشروع إلى أنظمة البنك تصديع كلمة المرور الخاصة بالدخول إلى البنك الإلكتروني (سواء الخاصة بالدخول إلى موقع البنك، أم الخاصة بالشبكة الداخلية للبنك). ويعود ذلك إلى أن العملاء عند قيامهم باختيار كلمة المرور الخاصة بهم للدخول على موقع البنك غالبا ما يختارون كلمات ضعيفة؛ أي سهلة التخمين بالنظر إلى شخصية صاحبها كما لو كانت كلمة المرور هي رقم تليفونه، أو اللجوء إلى قاموس يساعد المعتدى على التخمين(٣).

---

(1) **Password cracking,** Article , available at: http://www.webOpedia.com/TERM/P/ password_cracking.html

(٢) ويستعين المعتدون ببعض الأجهزة التي تقوم بإنتاج كمية كبيرة من كلمات المرور في ضوء أنشطة وسلوكيات عملاء البنك الإلكتروني؛ حيث يقومون بتتبع الكلمات التي يكثر استخدامها في الحياة اليومية لهؤلاء العملاء، أو الاستعانة بمعاجم اللغة المتخصصة في هذا الأمر. أ. **حسن مظفر الرزو**، مرجع السابق، ص٧٢.

(3) **Michael P. Dierks**; Op. Cit, p. 311; **Hackers** Article , available at: http://csrc.nist.gov/ publica-

ب- استغلال وجود خطأ في نظام تشغيل أجهزة وبرامج البنك الإلكتروني:

وجود أخطاء أو أعطال في نظام عمل البنك الإلكتروني أو نظام التشغيل الخاص بأحد التطبيقات المتعلقة بالعمليات المصرفية الإلكترونية من شأنه أن يجعل الفرصة سانحة ومهيأة أمام المعتدى للدخول غير المشروع على شبكة البنك الداخلية؛ حيث إن هذا العطل هو بمثابة نقطة ضعف في نظام الأمن الخاص بالبنك، يستغلها المعتدى كمنفذ دخول خاص لنظم البنك الداخلية. والمثال على ذلك لو أن سجل الفحص (Audit logs) الخاص بتسجيل بيانات عملية الدخول إلى البنك أصيب بعطل جعله يتوقف عن تسجيل بيانات الدخول الخاصة بالعملاء، على نحو هيأ الفرصة للدخول غير المشروع إلى البنك من قبل غير العملاء، أي دون الخضوع لإجراءات التوثيق والتدقيق التي يخضع لها أي شخص يرغب في التعامل مع البنك. أيضا لو أن إعداد وترتيب خطوات وإجراءات الدخول إلى موقع البنك الإلكتروني، أو إلى أحد التطبيقات المصرفية غير منظمة أو غير مؤمنة[1].

ج- تقليد الموقع الإلكتروني للبنك على شبكة الإنترنت Spoofing Web Bank:

يعد تقليد موقع البنك على شبكة الإنترنت من الطرق الأكثر شيوعا للدخول

---

tions/nistir/threats/subsection3_4_2.html.

(1) **CMS information systems threat identification resource**, available at: http://csrc. nist.gov/fasp/FASPDocs/risk-mgmt/Threat_ID_resource.pdf; **E-Banking,** Federal financial institutions examination council; Op. Cit, p. 27.

غير المشروع لموقع البنك الإلكتروني وهذه الطريقة كما سبق أن ذكرنا تتضمن قيام المعتدين بتصميم موقع مماثل لموقع البنك كوسيلة لغش العملاء، وخديعتهم بأن هذا هو موقع البنك الحقيقي، ومن ثم يتسنى لهم الحصول على البيانات الخاصة بالتعامل مع البنك من أجل استعمال هذه البيانات في الدخول غير المشروع على موقع البنك(١).

٤- الإجراءات الوقائية ضد اقتحام النظام الداخلي للبنك:

٢٧٩- تبدو أهمية التعرض للإجراءات الوقائية التي يجب على البنك اتخاذها للحيلولة دون وقوع الدخول غير المشروع، في بيان طبيعة الالتزامات القانونية الواقعة على عاتق البنك بخصوص تأمين موقعه الإلكتروني، وتأمين معاملاته المصرفية على شبكة الإنترنت(٢). يضاف إلى ذلك أن مثل هذه الإجراءات بمثابة توجيهات رقابية يلتزم بها البنك تجاه جهة الرقابة. وتوجد بعض الطرق الوقائية التي يمكن أن يلجأ إليها البنك الإلكتروني لتجنب حدوث ذلك، ومنها(٣):

أ- تأمين مكونات البنك الإلكتروني المادية والمعنوية. فيجب على البنك الإلكتروني أن يحيط كل أجزاء الشبكة ومكوناتها من أجهزة وبرامج ووسائل ربط الشبكة بسياج أمني مناسب يكفل عدم الدخول غير المشروع.

ب- يجب على البنك الإلكتروني أن يجرى فحصا دوريا لكل مكونات الشبكة وما

---

(١) راجع سابقا، بند ٥٢٥.

(2) **Background report on electronic commerce** 1998; Op. Cit, p. 54.

(3) **Satoru Torii, Yoshiki Higashikado, Takayoshi Kurita**, Framework of web applications for protection against illegal access, Fujtsu, June 2004, p. 103.

تتضمنه من بيانات لاكتشاف أي إتلاف أو تعديل يكون قد وقع، وإعداد تقارير مفصلة عن ذلك، ومحاولة إصلاح أي خلل يحدث وتحديد مسئولية من تسبب فيه.

ج- يجب على البنك الإلكتروني أن يزود نظام الدخول على شبكة البنك الداخلية بوسائل حماية خاصة، وذلك من خلال وضع أرقام تعريف خاصة أو اللجوء إلى نظم تشفير قوية[1].

٥- مسئولية مقتحم النظام الإلكتروني للبنك:

٢٨٠ - يستدعى الحديث عن مسؤولية مقتحم النظام الإلكتروني للبنك التعرض لمسؤوليته الجنائية والمدنية على النحو التالي:

أولا: المسئولية الجنائية لمقتحم النظام فى مواجهة البنك:

٢٨١- يثور التساؤل عن مسؤولية مقتحم النظام الإلكتروني للبنك، هل يعد جريمة في حد ذاته تنشأ معه مسؤولية المعتدى جنائيا، أم يلزم أن يترتب على هذا الاقتحام استعمال النظام بصورة غير مشروعة؟

بداية نود الإشارة إلى أنه لا يوجد نص خاص في قانون العقوبات المصري يجرم الدخول غير المشروع إلى أنظمة البنك الإلكتروني العامل عبر شبكة الإنترنت، كما أن نصوص الجرائم التقليدية في هذا القانون غير قادرة على أن تستوعب هذه الصورة من صور الانتهاكات. فلا يمكن القول مثلا بسريان نص

---

(1) **Graham Smith**; Op. Cit, p. 278.

المادة ٣٧٠ من قانون العقوبات[١] الخاصة بحماية وصيانة حرمة المكان الخاص (المسكن) ضد دخولها بقصد ارتكاب جريمة على حالة الدخول غير المشروع على أنظمة البنك الإلكتروني العامل عبر شبكة الإنترنت؛ حيث لا يسرى على الموقع الإلكتروني وصف المسكن، وما تقتضيه حرمته من سرية وخصوصية. كذلك لا مجال لإعمال نص المادة ٣٦٩ من ذات القانون والخاصة بحماية العقارات ضد الدخول غير المشروع لارتكاب جريمة داخل هذا العقار[٢]، حيث إن أنظمة الكمبيوتر لا تعد من قبيل العقارات، ومن ثم لا يسرى عليها هذا النص، وبناء عليه فإن الأمر يحتاج إلى ضرورة التدخل من المشرع المصري بنص خاص لتجريم الدخول غير المشروع إلى أنظمة البنك الإلكتروني العامل عبر شبكة الإنترنت وذلك على غرار التشريعات العقابية الأخرى.

وعن موقف التشريعات العقابية التي جرمت الدخول غير المشروع إلى أنظمة الكمبيوتر، فالملاحظ أن هناك تباينا في موقف هذه التشريعات على النحو التالي:

الاتجاه الأول: عدم الاكتفاء بمجرد الدخول غير المشروع:

ذهبت بعض التشريعات إلى عدم الاكتفاء بمجرد الدخول غير المشروع على أنظمة الكمبيوتر لوقوع الجريمة، حيث ذهب جانب منها إلى تطلب قيد خاص

---

(١) **وتنص هذه المادة** على أن " كل من دخل بيتا مسكونا أو معدا للسكن أو في أحد ملحقاته أو سفينة مسكونة أو في محل معد لحفظ المال وكانت هذه الأشياء في حيازة آخر قاصدا من ذلك منع حيازته بالقوة أو ارتكاب شيء مما ذكر، يعاقب بالحبس مدة لا تزيد على سنتين أو بغرامة لا تجاوز ثلاثمائة جنيه مصري".

(٢) **وتنص هذا المادة** على أن "كل من دخل عقارا في حيازة آخر بقصد منع حيازته بالقوة أو بقصد ارتكاب جريمة فيه أو كان قد دخله بوجه قانوني وبقى فيه بقصد ارتكاب شيء مما ذكر يعاقب بالحبس مدة لا تتجاوز ثلاثمائة جنيه مصري".

بالركن المعنوي لهذه الجريمة، هذا القيد متمثل في توافر قصد خاص لدى مرتكب الجريمة وهو قصد التأثير في البيانات الموجودة داخل أنظمة الكمبيوتر أو التأثير في أنظمة عمل هذه الأجهزة(١). ومن هذه التشريعات قانون العقوبات الألماني(٢)، والكندي(٣) والنمساوي(٤). والبعض الآخر من هذه التشريعات تطلب قيدًا خاصًا بالركن المادي للجريمة حيث تتطلب أن يتم هذا النشاط على نظم كمبيوتر خاصة بجهات معينة كالأجهزة الحكومية، أو أجهزة المؤسسات المالية(٥). ومن هذه القوانين القانون الفيدرالي الأمريكي الخاص بالغش وإساءة استعمال الكمبيوتر الصادر عام ١٩٩٤ (The Computer Fraud and Abuse Act, 18 U.S.C. section 1030)(٦).

الاتجاه الثاني: تجريم مجرد الدخول غير المشروع:

على الصعيد المقابل تبنت بعض التشريعات العقابية اتجاها آخر في هذا الصدد، حيث ذهبت إلى تجريم مجرد الدخول غير المشروع على أنظمة

---

(١) **د. شيماء عبد الغنى محمد عطا الله**،مرجع السابق، ص ٩٥.

(٢) هذا القانون متاح على العنوان الإلكتروني التالي:

http://wings.buffalo.edu/law/bclc/germind.htm

(٣) هذا القانون متاح على العنوان الإلكتروني التالي:

http://laws.justice.gc.ca/en/C-46/

(٤) هذا القانون متاح على العنوان الإلكتروني التالي:

http://query.nytimes.com/gst/abstract.html?res=9901E0DC173DE43BBC4D53DFB467838F669FDE

(5) **David L. Baumer and others**; Op. Cit, p. 407.**Katyal, Neal Kumar**; Op.Cit,p 40;**Michael P. Dierks**; Op. Cit, p. 327.

(٦) هذا القانون متاح على العنوان الإلكتروني التالي:

http://www.panix.com/~eck/computer-fraud-act.html

الكمبيوتر، مادام أن هذا الدخول قد تم دون رضاء صاحب هذه الأجهزة. من هذه القوانين قانون العقوبات الفرنسي، حيث نصت المادة ٣٢٣-١ منه على أن " يعاقب على الدخول أو الاستمرار في البقاء في نظام المعالجة الآلية للبيانات(١) أو جزء منه - بقصد الغش- بالحبس مدة لا تزيد على سنة والغرامة التي لا تزيد على ١٠٠ يورو". وقد نصت الفقرة الثانية من ذات المادة على "أن تشدد العقوبة في حالة إذا ما ترتب على هذا الدخول محو أو تعديل في البيانات المبرمجة في الجهاز بالحبس مدة لا تزيد على ٢٠٠ ألف يورو"(٢) أيضا جرم قانون العقوبات السويدي مجرد الدخول غير المشروع على مناطق معالجة البيانات(٣).

ويتضح من موقف المشرعين الفرنسي والسويدي أنهما جرما الدخول غير المشروع إلى النظام، يستوي في ذلك أن يكون الشخص الذي قام بالدخول غير مصرح له أصلا بالدخول، أو أنه مصرح له بذلك، ولكن تجاوز الحدود المسموح له الوصول إليها بسوء نية(٤) (وذلك كما لو قام أحد العاملين لدى البنك بالدخول

---

(١)هذا القانون متاح على العنوان الإلكتروني التالي:

http://www.legifrance.gouv.fr/html/codes_traduits/code_penal_textan.htm

- وقد عرفت لجنة القوانين بمجلس الشيوخ نظام المعالجة الآلية للبيانات بأنه كل مجموعة مركبة من وحدة أو عدة وحدات للمعالجة سواء كانت متمثلة في ذاكرات الحاسب وبرامجه ووحدات الإدخال، والإخراج والاتصال التي تساهم في نتيجة معينة وأن هذا المجموع من الوحدات يكون محميا بجهاز للأمن. د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني، دار النهضة العربية، ١٩٩٢، ص٤٢.

(٢) المرجع السابق، ص١١٢.

(٣) د.عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ص٣٠٩.

(٤) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول (الجرائم الناشئة عن استخدام الحاسب الآلي)، الطبعة الأولى، دار النهضة العربية،

إلى أجهزة أو ملفات خارج نطاق اختصاصه، أو أحد عملاء البنك الإلكتروني الذي استغل وجوده على موقع البنك، وتطرق إلى ملفات ليس له الحق في الوصول إليها)

- **رأينا الخاص:**

ونحن من جانبنا نؤيد موقف المشرع الفرنسي في هذا الصدد، حيث إنه نظر لجريمة الدخول غير المشروع على أنظمة الكمبيوتر على أنها جريمة نشاط (أو تعريض للخطر)(١)، وليست جريمة ضرر. فالجريمة تكتمل أركانها وعناصرها لمجرد الدخول غير المشروع، بغض النظر عما قد يترتب على هذا الدخول من نتائج. ويعود تأييدنا لموقف المشرع الفرنسي إلى تقديره لمدى خطورة النشاط المتمثل في الدخول غير المشروع على أنظمة البنك، حيث إن النشاط في حد ذاته كاف لأن يهدد أمن وسلامة نظم البنك وما تحتويه من بيانات، فالدخول بدون مراعاة التعليمات والإرشادات الأمنية أمر يشكل خطورة وتهديدًا لأمن البنك، حتى ولو لم يصل الأمر إلى حد المساس بالبيانات. فهذا الخطر في حد ذاته نتيجة يجب أن يعاقب عليها القانون.

ومما يؤكد خطورة مجرد الدخول غير المشروع أيضا قيام بعض البنوك

١٩٩٢، ص١٥٠.

(١) ويعرف التعريض للخطر بأنه عبارة عن سلوك إنساني منشئ لحالة الخطر يعني احتمال حدوث ضرر بالمصلحة التي يحميها القانون. وقد تبنت التشريعات العقابية مفهوم جرائم التعريض للخطر استجابة لما شهدته الوسائل الفنية الحديثة من تطور وتقدم، حيث يكتفي فيها المشرع بأن يترتب على السلوك الإجرامي خطر يهدد المصلحة المراد حمايتها، دون استلزام الإضرار الفعلي، فهذا الخطر هو بذاته نتيجة يعاقب عليها القانون. انظر د. **أحمد شوقي عمر أبو خطوة**، مرجع سابق، ص ١٩٣ وما بعدها.

العاملة عبر شبكة الإنترنت بعدم السماح بالدخول حتى على الموقع الإلكتروني للكافة، بل يقتصر الأمر على عملاء البنك الحاملين لكلمة المرور الخاصة بالتعامل مع البنك، ومن ثم يعد مجرد الدخول غير المشروع على أنظمة البنك جريمة. يضاف لكل ذلك أن الدخول غير المشروع على أنظمة البنك يحمل بين طياته اقتراب وقوع الاعتداء الفعلي على البيانات الموجودة داخل هذه الأنظمة، على نحو يمكن معه النظر إلى هذا النشاط على أنه بدء في تنفيذ هذه الجريمة (وفقا للمعيار الشخصي) يمكن أن يعاقب عليه حتى ولو لم يصل الأمر إلى حد المساس بالبيانات الموجودة على الموقع.

وحسنا فعل المشرع الفرنسي حين ألحق فقرة ثانية في ذات المادة قرر خلالها ظرفا مشددا لهذه الجريمة إذا ترتب على هذا الدخول غير المشروع محو أو تعديل في البيانات المبرمجة في الموقع، حيث إن ذلك من شأنه أن يزيد من مستوى الحماية المقرر لأنظمة الكمبيوتر وما تتضمنه من بيانات.

وبناءً عليه فإن مجرد الدخول غير المشروع على موقع البنك الإلكتروني العامل عبر شبكة الإنترنت يشكل في حد ذاته جريمة يسأل عنها المعتدى جنائيا في مواجهة البنك الإلكتروني.

ثانيا- المسئولية المدنية لمقتحم النظام الداخلي للبنك:

٢٨٢- تنعقد المسؤولية المدنية للمهاجم عن الدخول غير المشروع في مواجهة كل من البنك وعميله على التفصيل التالي:

أ- المسؤولية المدنية للمقتحم في مواجهة البنك:

يسأل المقتحم مدنيا في مواجهة البنك الإلكتروني في حالة ثبوت ارتكابه

لجريمة الدخول غير المشروع على موقع البنك بحكم نهائي يصدر بذلك من المحكمة المختصة، وذلك بموجب قواعد المسئولية التقصيرية، والتي تقرر "أن كل خطأ سبب ضررا للغير يلزم مرتكبه بالتعويض"(١).

ويجب على المحكمة عند تقدير التعويض المستحق للبنك الإلكتروني، أن تراعى مقدار الضرر الذي لحق البنك من جراء الدخول غير المشروع على نظمه الداخلية، والتي ترتب عليها انتهاك خصوصيته، والتعدي على أمنه، خاصة ما يتعلق بالضرر الأدبي الذي يلحق بسمعة البنك من جراء ذلك، والذي ينعكس سلبا على ثقة العملاء فيه.

ب- المسؤولية المدنية للمقتحم في مواجهة العميل:

من خلال تدقيق النظر في نشاط المعتدى، والمتمثل في مجرد الدخول غير المشروع على نظم البنك الإلكتروني الداخلية، نلاحظ أن هذا النشاط وإن كان يمثل خطأ من قبل المعتدى، إلا أن ضرره لا يلحق بعملاء البنك الإلكتروني بصورة مباشرة، على نحو يمكن معه القول إنه لا مجال لرجوع عملاء البنك الإلكتروني على المعتدى في هذه الحالة، كل ذلك ما لم يتطور نشاط المعتدى من مجرد الدخول غير المشروع إلى أنشطة أخرى تشكل اعتداءً على حقوق العملاء بصورة مباشرة.

---

(١) انظر المادة ١٦٣ من القانون المدني المصري.

المطلب الرابع

سرقة البيانات الشخصية لعملاء البنك الإلكترونى

(Identity Theft) [1]

٢٨٣- تشكل البيانات الشخصية (personal information)[2] لعملاء البنك الإلكتروني أهمية كبيرة، سواء بالنسبة للعملاء أم بالنسبة للبنك الإلكتروني. فالعملاء يعتمدون على هذه البيانات بصورة كبيرة في إتمام معاملاتهم المصرفية مع البنك عبر شبكة الإنترنت، حيث يستخدمون هذه البيانات في الدخول على

---

(١) تعد سرقة البيانات الشخصية من أكثر الجرائم التي ترتكب عبر شبكة الانترنت، حيث قدر مركز التجارة الفيدرالي الأمريكي (FTC) عدد جرائم سرقة البيانات التي ترتكب سنويا بحوالي ٩ مليون حالة. كذلك سجل هذا النوع من الجرائم رقما مرتفعا في بريطانيا حيث بلغ عدد القضايا ١٣٧٠٠٠ قضية في عام ٢٠٠٥ وقدرت وزارة الداخلية (Home office) الخسائر المترتبة على ذلك بنحو ١,٧ بليون إسترليني.

Fighting back against, Identity theft, available at:
http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

Online identity theft, Security report, February 2006, available at:
www.btplc.com/onlineidtheft/onlineidtheft.pdf

(٢) ويجب أن نلاحظ أن هناك فرقا بين البيانات الشخصية والبيانات الخاصة، حيث تتميز الأولى بأنها أكثر شمولية من الثانية، فليست كل البيانات الشخصية بيانات خاصة، حيث تتميز الأخيرة انها أكثر سرية وخصوصية. فرقم تليفون المنزل يعد من قبيل البيانات الشخصية، لكن هذا لا يمنع من إمكانية إطلاع الكافة عليه من خلال وضعه في دليل عام للتليفونات، ومن ثم لا يعد من البيانات الخاصة، فالأخيرة تتميز بأن جانب الخصوصية والسرية فيها يزيد، وذلك إلى الحد الذي يجعل صاحب البيانات الخاصة لا يطلع عيها إلا القليل.

David L. Baumer and others; Op. Cit, p. 403

الموقع الإلكتروني للبنك، والوصول إلى حساباتهم الشخصية والتحكم في كل ما يتعلق بها من تعاملات، أيضا يعتمدون على هذه البيانات في تقديم الطلبات الخاصة بإجراء المعاملات المصرفية عبر الشبكة[1]. أما بالنسبة للبنك الإلكتروني فتعاملاته مع العملاء تتم عن بعد، لذلك فهو يعتمد على هذه البيانات بشكل أساسي للتعرف على شخصية عملائه، ومن ثم التجاوب معهم بخصوص المعاملات المصرفية، ومن ثم فإن البيانات الشخصية لعملاء البنك تشكل أهمية بالنسبة للعملاء والبنك، الأمر الذي يجعل سرقة هذه البيانات لا تمس أمن العميل وحده، ولكن أمن البنك الإلكتروني أيضا[2]. ويقتضى الامر على هذا النحو التعرض لتعريف البيانات الشخصية فى نظام عمل البنك، ومدى إعتبار هذه البيانات من قبيل الاسرار المصرفية، وتحديد المقصود بسرقة البيانات الشخصية، وكيفية سرقة هذه البيانات، والاجراءات اللازمة للحيلولة دون وقوع هذا الاعتداء، والمسؤلية القانونية عنها، وذلك على النحو التالى:

١- تعريف البيانات الشخصية:

٢٨٤- تبدو أهمية التعرف على ماهية البيانات الشخصية؛ وذلك باعتبارها محل جريمة سرقة البيانات الخاصة بعميل البنك، والتي يسفر عن سرقتها الكثير من

---

(1) **Jyske bank**, JBPB, Net bank user agreement, (EN)-2007, available at:
http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf

(2) **Anna Granova & JHP Eloff**, Online banking and identity theft: who carries the risk?, Computer& farud security, (without published date), p. 7; **Zakaria I. Saleh**; Op, Cit, p. 9; **Authentication in an Internet Banking Environment**; Op. Cit, p. 5.

المشاكل الأمنية. الأمر الذي يدعو للتعرف عليها، لتوفير الحماية القانونية المناسبة لها. أيضا يعد التعرف على هذه البيانات تمهيدا للإجابة عن تساؤل يتعلق بمدى اعتبار هذه البيانات من قبيل الأسرار المصرفية.

هذا وقد خلا النظام القانوني المصري من وضع تعريف للبيانات الشخصية، سواء على صعيد المعاملات التقليدية أم الإلكترونية، وسواء على صعيد المعاملات المصرفية أو غيرها من المعاملات.

أما على صعيد التشريعات الأخرى، فالملاحظ أن هناك اتجاهين في تعريف البيانات الشخصية للمعاملات عبر شبكة الإنترنت، وذلك على النحو التالي:

الأول- اتجاه مضيق:

وقد تبنى التوجيه الأوربي الخاصة بحماية البيانات الشخصية(١) هذا الاتجاه حيث عرف هذه البيانات بأنها عبارة عن "أية معلومات تتعلق بتمييز شخص طبيعي".

والملاحظ أن هذا التوجيه قد ضيق من مفهوم هذه البيانات حيث قصرته فقط على المعلومات المستخدمة في تمييز وتحديد شخص صاحبها.

الثاني- اتجاه موسع:

وقد تبنى هذا الاتجاه القانون الأمريكي لحماية سرية البيانات على شبكة الإنترنت(online privacy protection Act 2003) (٢)، حيث عرف هذه

---

(1) **Directive EC,** 95/46/, Official Journal of the European Communities chapter 1, article 2.

(٢) هذا القانون متاح على العنوان الإلكتروني التالي:

البيانات في المادة الثامنة منه بأنها عبارة عن البيانات التي تحدد شخصية صاحبها ككلمة المرور (password) الخاصة بالدخول على حساب العميل وأرقام بطاقة الائتمان وأرقام الحساب الخاص بهذا العميل، والمعلومات التي يمكن التوصل إليها باستخدام هذه البيانات.

والملاحظ على القانون الأمريكي أنه تبنى تعريفا موسعا لما يقصد بالبيانات الشخصية، فلم يقصرها على العبارات المستخدمة في التعامل مع البنك، ولكن ضم إليها البيانات المحمية بهذه العبارات. فوصف البيانات الشخصية من وجهة نظر هذا القانون لا يقتصر على العبارات والأرقام والاختصارات المستخدمة في تعريف الشخص، ولكن تمتد إلى البيانات التي تستخدم هذه العبارات للوصول إليها.

ويبدو لنا رجحان موقف القانون الأمريكي في هذا الخصوص؛ فهذه الرموز والاختصارات أنما تستمد قيمتها من قيمة المعلومات التي تحميها، وذلك على النحو الذي يجعل صاحب هذه العبارات ليس حريصا عليها لذاتها ولكن لما تحميه من بيانات. يضاف إلى ذلك أن هذا التعريف يتلاءم مع وحدة مفهوم أمن البنك وعميله، وذلك على النحو الذي يجعل الاعتداء على هذه البيانات اعتداءً على أمن البنك أيضا.

وتتميز البيانات الخاصة بعملاء البنك بأنها غير مرتبطة بشخصية صاحبها، وذلك على عكس الخواص البيومترية (مثل بصمة الأصابع، اتساع حدقة العين، درجة تردد الصوت) الأمر الذي يسمح باستعمال هذه البيانات من قبل صاحبها،

---

http://www.kronishlieb.com/files/tbl_s24News%5CPDFUpload152%5C927%5CALERT-Cal_OPPA.pdf

أو غيره ممن يعلمون بها(١).

وبعد التعرف على المقصود بالبيانات الشخصية، يثور تساؤل يتعلق بمدى اعتبار هذه البيانات من قبيل الأسرار المصرفية؟

٢- مدى اعتبار البيانات الشخصية لعميل البنك الإلكتروني من قبيل الأسرار المصرفية:

٢٨٥- تتطلب الإجابة على هذا التساؤل التعرف على المقصود بالسر المصرفي لدى التشريعات القانونية، وأحكام القضاء وآراء الفقه، وذلك على النحو التالي:

أ) التعريف التشريعي:

خلت التشريعات المصرية وما ظهر لنا من التشريعات المصرفية المقارنة(٢) من وضع تعريف للمقصود بالسر المصرفي بصورة عامة، والسر المصرفي على شبكة الإنترنت بصورة خاصة. فعلى الرغم من حرص هذه التشريعات على التأكيد والتشديد على حماية السر المصرفي، إلا أنها مع ذلك لم تضع تعريفا يبين ماهيته.

ويعد السكوت التشريعي في مجال وضع التعريفات أمرا محمود، نظرا لما

---

(1) **Identity Theft and Identity Fraud**, available at:

http://www.usdoj.gov/criminal/fraud/websites/idtheft.html

(٢) راجع أمثلة على هذه القوانين على العناوين الإلكترونية التالية:

http://www.lexinter.net/Legislation2/atteinte_au_secret_professionnel.htm

http://www.gpoaccess.gov/uscode/browse.html

يترتب على هذا التدخل من صعوبات تتعلق بضيق النصوص وعجزها عن ملاءمة الواقع، خاصة إذا ما كان الأمر يتعلق بالمعاملات المصرفية الإلكترونية، تلك التي تتسم بالتطور الشديد. لكن يبدو لنا أن هناك طريقا آخر يمكن للمشرع أن يسلكه في هذا الصدد؛ وهو ذكر أهم الخصائص التي تميز الأمر المراد تعريفه (السر المصرفي في المعاملات الإلكترونية)، وذلك حتى يمهد الطريق وييسره أمام القضاء وهو بصدد التعرض لمنازعات تتعلق بهذا الأمر، خاصة في ظل ما تتسم به المعاملات المصرفية الإلكترونية من حداثة، وغلبة الطابع الفني، وعدم استقرار العرف بشأن تحديد ماهية السر المصرفي بشأنها.

ب) التعريف القضائي:

وعلى صعيد الأحكام القضائية، نلاحظ أيضا وجود ندرة نسبية في الأحكام القضائية التي تعرضت لهذا الأمر، بل حتى ما ظهر لنا من أحكام للقضاء الفرنسي في هذا الخصوص بينها تضارب في تعريف السر المصرفي بصورة عامة.

فقد ذهب أحد الأحكام في تعريفها للسر المصرفي بأنها البيانات التي تعتبر سرا نظرا لطبيعتها الخاصة، التي تفرض عدم اطلاع الغير عليها لاتصالها بخصوصيات صاحبها. وأضاف هذا القضاء أنه لا يؤثر في مفهوم السر المصرفي على النحو السابق أن يطلب صاحبه اعتباره سرا[1]. هذا من ناحية.

ومن ناحية أخرى ذهبت أحكام أخرى للقضاء الفرنسي تعرف السر المصرفي بأنه تلك البيانات التي يطلب صاحبها اعتبارها سرا، وذلك بمنع اطلاع

---

(1) Cass.5 juillet 1893. Dalloz

الغير عليها، أو حصر الاطلاع عليها على أشخاص محددين[١].

وقد ذهب بعض الفقه[٢] في سبيل تحديده لطبيعة ونطاق السر المصرفي إلى أنه عبارة عن حق أو مصلحة خاصة Private interest يتم تحديد ماهيته ونطاقه بمعرفة الاتفاقات الخاصة بين الأطراف المتعاقدة بما يحقق مصالحهم المشتركة. وقد برر هذا الفقه ذلك بأن السر المصرفي لا يعد واجبا مطلقا على البنك، بل أن القانون يفرض عليه في بعض الحالات الإدلاء بالسر المصرفي لاعتبارات يقدرها. ولعل هذا الاتجاه الفقهي في تحديد طبيعة السر المصرفي يبرر لنا عدم وجود تشريعات تعرف السر المصرفي، وقلة الأحكام القضائية في هذا الخصوص، حيث يترك الأمر ليحدد بمعرفة الاتفاقات الخاصة بين البنك وعميله.

ج) التعريف الفقهي:

وعن موقف الفقه في هذا الخصوص، نلاحظ وجود اختلاف بين الفقه في تعريف السر المصرفى، وذلك على النحو التالي:

فذهب اتجاه يعرفه[٣] بأنه عبارة عن البيانات المحددة الخاصة بالعميل، كرقم مبلغ رصيد الاعتمادات المفتوحة ومواعيد استحقاق ديونه وأرقام ميزانيته، وتقديمه طلبا بتأجيل وفاء الديون التي عليه، وما إذا كان له حساب لدى البنك أم

---

(1) **Siret** 1896-184. Dalloz

مشار إلى هذه الأحكام لدى محمد عبد الحي إبراهيم سلامة، إفشاء السر المصرفي بين الحظر والإباحة، رسالة دكتوراه، كلية الحقوق - جامعة المنصورة، ٢٠٠٤، ص ٢٠.

(٢) **د. سعيد عبد اللطيف حسن**، الحماية الجنائية للسرية المصرفية، دار النهضة العربية، ٢٠٠٤، ص ٢٣٥.

(٣) **د. على جمال الدين عوض**، مرجع سابق، ص ١٠٨٤.

لا.

ولعل هذا التعريف وضعنا أمام تساؤل آخر يتعلق بماهية البيانات المحددة، وذلك على اعتبار أن ما ذكره من بيانات هي مجرد أمثلة للبيانات المحددة وليس حصرا لها.

وذهب اتجاه آخر(١) إلى تعريف السر المصرفي بأنه عبارة عن "الأسرار المستودعة لدى بنك له مركز أو وضع خاص في نظر القانون".

والملاحظ على هذا التعريف، أنه عرف الشيء بنفسه؛ حيث استخدم في التعريف كلمة السر، أيضا تبنى مفهوما واسعا للسر المصرفي، حيث إنه يشمل كل ما يتم استيداعه لدى البنك من بيانات خاصة بالعميل.

- رأينا الخاص:

يبدو لنا ونحن بصدد تعريف السر المصرفي بصورة عامة في ضوء موقف التشريعات، وأحكام القضاء، وآراء الفقه سابقة الذكر أن فكرة السر المصرفي فكرة مستعصية على الحصر والتحديد؛ ويعود ذلك إلى أن فكرة السر المصرفي فكرة نسبية تختلف من شخص لأخر بحسب النطاق الذي يحدد من خلاله كل شخص حدود حياته الخاصة، والأشخاص المخول لهم الاطلاع على بياناته الخاصة، كما تختلف هذه الفكرة من بنك لآخر بحسب طبيعة معاملاته المصرفية، وبحسب النظام القانوني لدولة البنك، ومدى تبنيها لتشريعات تبالغ في حماية الحياة الخاصة لأفرادها أم لا تبالغ .

يضاف إلى ذلك طبيعة العرف المصرفي السائد في دولة البنك، والذي يلعب

---

(١) **د. سعيد عبد اللطيف**، مرجع سابق، ص ٢٠٥.

دورا كبيرا في تحديد مضمون السر المصرفي، يضاف أيضا إلى أسباب صعوبة حصر هذه الفكرة التطور المستمر والمتلاحق لمعاملات البنوك، خاصة بعد ولوجها عصر المعلومات، وقيام معاملاتها بصورة كبيرة على التبادل الإلكتروني للبيانات.

وإذا كان من الممكن أن نجتهد في هذا الأمر لمحاولة تقريب الرؤية قدر الإمكان، فأننا نقترح أن يعرّف السر المصرفي بأنه عبارة عن مجموعة البيانات التي تتصل بالحياة المالية الخاصة بالعميل، والتي تتحدد في ضوء ما يتم الاتفاق عليه بين البنك وعميله، وفى ضوء ما استقر عليه العرف المصرفي.

ويلاحظ أن هذا التعريف يبرز خصائص السر المصرفي، وهى:

- أن السر المصرفي يشتمل على كافة البيانات الخاصة بالمعاملات المالية للعميل مع البنك، دون تحديد لهذه البيانات، وذلك لتغطية كافة أنواع البيانات التي قد يفرزها التطور في المعاملات المصرفية.
- أن السر المصرفي في علاقة البنك والعميل مسألة نسبية تختلف من بنك لآخر ومن عميل لآخر، ويستعان في تحديد نطاقها باتفاق البنك والعميل، والعرف المصرفي السائد.

والتساؤل: هل يختلف مفهوم السر المصرفي للمعاملات المصرفية على شبكة الإنترنت عن مفهوم السر المصرفي بصورة عامة؟

لم يظهر لنا من مطالعة التشريعات القانونية وأحكام القضاء المختلفة أنها تتبنى مفهوما مختلفا للسر المصرفي للمعاملات الإلكترونية عن مفهوم السر المصرفي بصورة عامة.

ونحن من جانبنا لا نرى اختلافا في مضمون السر في كل من الحالتين؛ فكلاهما عبارة عن مجموعة البيانات التي تتصل بالحياة المالية الخاصة بالعميل، والتي تتحدد في ضوء ما يتم الاتفاق عليه بين البنك وعميله، وفي ضوء ما استقر عليه العرف المصرفي.

لكن الاختلاف يتجلى في نطاق كل منهما: فإذا كانت النظرة التقليدية التي سادت السر المصرفي بصورة عامة كانت تقوم على أن السر المصرفي التزام مهني يقع على البنك فقط، لكن في ظل نظام البنوك العاملة على شبكة الإنترنت، أصبح لعميل البنك نصيب من هذا الالتزام؛ حيث في إطار التعامل عن بعد عبر شبكة دولية للاتصال يقوم البنك بتزويد العميل ببعض البيانات الخاصة التي تسمح له بالدخول على الموقع الإلكتروني للبنك والتعامل معه، ويحرص البنك في إطار تأمين موقعه الإلكتروني وتعاملاته بصورة عامة أن يلزم العميل بضرورة الحفاظ على سرية هذه البيانات، والاستعمال الشخصي لها نظرا لأهمية هذا الأمر وخطورته بالنسبة للبنك، الأمر الذي يجعل العميل هو الأخر مخاطبا بأحكام السرية المصرفية، نظرا لأن هذه البيانات تؤثر بصورة مباشرة في أمن البنك بصورة عامة.

ونخلص من كل ذلك إلى أن البيانات الشخصية بالمفهوم السابق ذكره تعد من قبيل الأسرار المصرفية في علاقة البنك الإلكتروني بعميله، فالبيانات الشخصية بهذا المفهوم ليست فقط بيانات لتعامل العميل مع البنك عن بعد عبر شبكة الإنترنت، ولكنها بيانات مالية، وذلك بالنظر إلى ارتباطها الشديد والمباشر بحسابات العميل وكافة معاملاته المصرفية على شبكة الإنترنت، لذلك تعد البيانات الشخصية من قبيل الأسرار المصرفية.

٣- تعريف سرقة البيانات الشخصية لعميل البنك الإلكتروني:

٢٨٦- عرف بعض الفقه[١] سرقة بيانات المتعاملين على شبكة الإنترنت بأنها عبارة عن " سوء استخدام البيانات الشخصية لشخص آخر، مثل الاسم وتاريخ الميلاد وعنوان البريد الإلكتروني، وذلك بدون علمه أو موافقته.

وعرفت أيضا[٢] بأنها عبارة عن استخدام البيانات الخاصة بشخص ما (والتي تستخدم لتميزه)، مثل الاسم ورقم الضمان الاجتماعي ورقم بطاقة الائتمان، بدون رضاه للاحتيال أو ارتكاب الجرائم الأخرى.

وعرفت كذلك[٣] بأنها عبارة عن اختراق أجهزة الحاسب الآلي المرتبطة بشبكة الإنترنت بقصد سرقة معطياتها والبيانات المخزنة فيها، مثل اختراق شبكات المصارف المالية والبنوك لعمل تحويلات مصرفية غير مشروعة.

والملاحظ على مجموع هذه التعريفات أنها لا تنظر لسرقة البيانات الخاصة بالمتعاملين عبر شبكة الإنترنت على أنها مجرد الاستيلاء على هذه البيانات فقط، بل تتطلب أيضا استخدام هذه البيانات استخداما سيئا، وذلك من خلال قيام السارق بالتعامل بهذه البيانات على أنه صاحبها، بصورة تضر صاحبها الحقيقي، الأمر الذي يجعل نشاط هذه الجريمة نشاطًا مركبًا يتضمن الاستيلاء على البيانات ثم استعمالها استعمالا غير مشروع. فلا يكفى مجرد الاستيلاء لوقوع الجريمة بل يجب أن يقترن به الاستعمال غير المشروع لهذه البيانات.

---

(1) **Online identity theft**; Op. Cit,

(2) Fighting Back Against; Op. Cit.

(٣) د. محمد عبد الرحيم سلطان العلماء، مرجع سابق، ص١١.

ويبدو لنا أن هذه التعريفات لا تحقق الوصف الأمثل والملائم لسرقة البيانات الخاصة بالمتعاملين على شبكة الإنترنت بصورة عامة، والمتعاملين مع البنوك العاملة على هذه الشبكة بصورة خاصة، والذي يجب أن يتوقف عند حد الاستيلاء على هذه البيانات، حتى ولو لم يصل الأمر إلى استخدامها بصورة غير مشروعة. فمجرد التوصل لمعرفة هذه البيانات بدون علم ورضاء صاحبها هو سرقة لها، يستوى بعد ذلك استغلالها أو عدم استغلالها. هذا من ناحية.

ومن ناحية آخري، الاتجاهات الحديثة[1] تتجه إلى إضفاء وصف المال على البيانات ذات القيمة الاقتصادية بالنسبة لصاحبها، الأمر الذي يجد مجاله الخصب في التعاملات المصرفية، حيث تكتسب البيانات الخاصة بعميل البنك ذات أهمية المعاملات التي تستخدم فيها، وبناءً عليه يبدو لنا تعريف سرقة هذه البيانات كصورة من صور الانتهاكات التي تستهدف أمن البنك الإلكتروني بأنها عبارة عن "قيام أحد الأشخاص بالاستيلاء على البيانات الخاصة بعميل البنك والتي يستخدمها في التعامل مع البنك عبر شبكة الإنترنت".

٤- كيفية سرقة البيانات الشخصية لعملاء البنك الإلكتروني:

٢٨٧- هناك العديد من الطرق التي يلجأ إليها سارقو بيانات عملاء البنك الإلكتروني للتوصل إلى هذه البيانات واستخدامها بصورة غير مشروعة. والملاحظ على هذه الطرق أنها ليست مقصورة على تعاملات العميل عبر شبكة الإنترنت فقط، بل يمكن للسارق أن يتوصل إليها من خلال مراقبة نشاط العميل اليومي بصورة عامة، حتى يتسنى له التوصل إلى هذه البيانات ثم ممارسة

---

(١) د.عبد الله حسين محمود. مرجع سابق، ص ١٦٧.

نشاطه مع البنك عن طريق شبكة الإنترنت. ومن هذه الطرق[1]:

١- قيام المعتدين بإرسال رسائل بريد إلكتروني مزيفة إلى عميل البنك الإلكتروني، يصورونها على أنها قادمة من البنك، حيث يطلبون في هذه الرسائل إرسال كلمة المرور الخاصة بالعميل، أو أرقام الحساب الخاصة به، ويبررون ذلك مثلا بالرغبة في حذف هذه البيانات من قاعدة البيانات الخاصة بالبنك لوجود عطل ما[2].

٢- قيام المعتدين بتثبيت أجهزة تعمل على مراقبة سلوكيات العميل وتعاملاته مع كل الأدوات التي يمكن أن يستعملها للتواصل مع البنك، مثل الكمبيوتر الشخصي الخاص به، أو مكائن سحب النقود. وما قد لا يعلمه البعض أن الكمبيوتر الشخصي يقوم بجمع كل أنواع المعلومات الخاصة بهذا بالشخص الذي يستعمله، ويقوم بتخزين هذه المعلومات في ملفات خفية (hidden files) تحفظ على القرص الصلب الخاص بجهازه. هذه الملفات تحتوى على بيانات خاصة به مثل؛ كلمة المرور التي يستعملها، أرقام بطاقات الائتمان الخاصة به، عناوين المواقع التي يتردد عليها. ويتمكن المعتدى من الحصول على هذه البيانات بإحدى طريقتين: إما أن يقوم بالتقاط هذه البيانات أثناء إرسالها بطريقة غير مؤمنة، أو أن يقوم بتثبيت برنامج على الجهاز الخاص بالشخص الذي يريد سرقة بياناته الشخصية، بحيث يقوم هذا البرنامج بتجميع هذه البيانات وإرسالها بصورة آلية إلى الشخص الذي قام

---

(1) **Katyal, Neal Kumar**; Op. Cit, p. 45.

(2) **Identity Theft and Identity Fraud**, available at: http://www.usdoj.gov/criminal/ fraud/websites/idtheft.html

بتثبيت البرنامج(١).

٣- لجوء المعتدين إلى وسائل احتيالية، مثل قيامهم مثلاً بإنشاء موقع إلكتروني(٢)، والقيام بعرض منتجات أو خدمات وهمية من خلال هذا الموقع، ويطلبون من المتعامل إدخال تفاصيل خاصة باسمه، وعنوان بريده الإلكتروني، وأرقام حسابه المصرفي للحصول على السلعة أو الخدمة المعلن عنها، ثم يقومون باستغلال هذه البيانات بعد ذلك في التعامل مع البنك الإلكتروني.

٤- قيام المعتدين بالبحث في الأوراق، أو المستندات أو الفواتير الخاصة بعميل البنك الإلكتروني، عن تفاصيل خاصة ببياناته الشخصية، والتي يمكن استغلالها في التعامل مع البنك الإلكتروني(٣).

والسؤال: ماذا يمكن أن يفعل المعتدى بعد الحصول على البيانات الخاصة بعميل البنك الإلكتروني؟

٥- طرق استغلال البيانات الخاصة بالعميل الإلكتروني:

٢٨٨- بعد أن يحصل المعتدى على بيانات عميل البنك الإلكتروني، فإنه يقوم

---

(1) **Internet Identity Theft,** Article available at: http://www.winferno.com/guides/ articles/internet-identity-theft-email-fraud.asp

(2) **Tom Arnold,** Internet Identity Theft, Technology Working Group, e Business Division, June 2000, p. 7.

(3) **Online identity theft**, Security report, February 2006, www.btplc.com/onlineidtheft/onlineid**theft**.pdf; **Identity Theft and Identity Fraud,** available at:http://www.usdoj.gov/criminal/fraud/websites/idtheft.html

باستغلال هذه البيانات بما يحقق له فائدة، وعلى نحو يضر بالعميل صاحب هذه البيانات. ويمكن أن تأتي تصرفات المعتدى في هذه البيانات على النحو التالي:

الأولى: التحكم في الحساب "Account takeover":

يحدث هذا عندما يقوم المعتدى بعد الاستيلاء على كل البيانات الخاصة بحساب العميل باستخدام هذه البيانات للدخول على هذا الحساب عن طريق موقع البنك الإلكتروني على شبكة الإنترنت، والتعامل مع هذا الحساب باعتباره مالكا له من خلال إجراء تحويلات إلكترونية لنفسه أو للغير، كما يمكن أن يقوم بفتح حساب جديد بالأموال الموجودة في هذا الحساب باسمه، كما يمكن للمهاجم أيضا بعد الدخول على الحساب أن يغير من كلمة المرور الخاصة بالدخول عليه حتى يحرم صاحب الحساب الحقيقي من الدخول عليه أو التعامل به[1].

الثانية: اصطناع طلبات مزيفة "Application fraud":

يحدث هذا عندما يقوم المعتدى بالاستيلاء على كل البيانات الخاصة بالعميل، ثم يقوم باستغلال هذه البيانات، والتعامل بها وكأنه صاحبها، فيقوم مثلا بملء النماذج الخاصة بالحصول على السلع، والخدمات باستعمال هذه البيانات[2]، أو يقوم بالحصول على الخدمات المصرفية من البنك الإلكتروني باستعمال هذه البيانات على أنه صاحبها.

٦- الإجراءات الوقائية للحيلولة ضد سرقة بيانات عميل البنك

---

(1) **Reducing the Risk of Identity Theft**, Article available at : http://www.privacyrights. org/fs/fs17-it.htm

(2) **Tom Arnold;** Op. Cit, p. 7.

الإلكتروني:

٢٨٩- يقع على عاتق عميل البنك الإلكتروني عدة التزامات، تضمنتها بعض العقود الخاصة بالبنوك العاملة عبر شبكة الإنترنت، وأوجبت على العميل الالتزام بها من أجل ضمان عدم سرقة البيانات الخاصة بتعاملاته مع البنك، وذلك أثناء التعامل عبر شبكة الإنترنت بصورة عامة، وهي(١):

أ- ألا يترك العميل أي شخص ينفرد بجهاز الكمبيوتر الخاص به بأن يحمى الدخول على هذا الجهاز بكلمة مرور لا يعرفها إلا هو، وإذا سمح لأحد بالتعامل مع جهازه يجب أن يتم ذلك تحت إشرافه المباشر.

ب- يجب على العميل أن يتوخى الحرص الكافي عند تعاملاته على شبكة الإنترنت مع المواقع المختلفة، خاصة عند الإفصاح عن بياناته الشخصية(٢).

---

(1) **Internet Banking Security**; available at: http://www.eldersruralbank.com.au/internet-banking/internet-banking-security#internet_banking_security; **Jyske bank**, JBPB, Net Bank user agreement, (EN)-2007, available at: http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf

(٢) وقد جاءت جميع نماذج العقود المصرفية المعروضة على مواقع البنوك الإلكترونية على شبكة الانترنت تحرص على ضرورة استعمال بيانات التعريف الشخصية الخاصة به بحذر شديد، فيوصى مثلا بضرورة حفظ العميل لهذا الرقم في ذاكرته، ولا يحتفظ به في ورقة خارجية، أو إخبار أي شخص به.

(You will be given a PIN so you can carry out transactions using your card at ATMs and pay for goods and services electronically. You must memories your PIN immediately and destroy the notification promptly on receipt. You must keep your PIN secret. You must not tell anyone your number not even our staff or the police. You should never write down your PIN). See **Flex Account Terms**

وقد جاءت جميع نماذج العقود المصرفية المعروضة على مواقع البنك الإلكتروني على شبكة الإنترنت متضمنة ضرورة استعمال بيانات التعريف الخاصة بالعميل بحذر شديد، فيوصى مثلا بضرورة حفظ العميل لهذه البيانات في ذاكرته، ولا يحتفظ بها في ورقة خارجية، أو إخبار أي شخص بها، وأن يحرص دائما على التعامل مع المواقع التي تتبع إجراءات التوثيق، والتي تظهر سياستها الخاصة بالسرية بشكل واضح.

ج- أن يقوم العميل بتنظيف متصفح المواقع (web browser) الخاص به في كل مرة يقوم فيها بالدخول على موقع البنك، ويتأكد أنه لم يترك أي بيانات شخصية (مثل اسم المستخدم username أو كلمة المرور password) محفوظة على أي جهاز أو موقع(١).

د- أن يقوم العميل في حالة اكتشاف أي سرقة لبياناته الشخصية (كما لو وصل إليه من البنك كشوف بأشياء لم يقم بشرائها مثلا) بإبلاغ البنك الإلكتروني

---

and Condition, available at: http://www.nationwide.co.uk/internetbanking/help/help_FlexAccount_Terms_and_Conditions.htm; **HSBC**, Terms and Conditions for Internet Banking, available at: http://www.bahrain.hsbc.com/public/meregional/bahrain_hom/pOpups/en/bah_pib_ terms.jhtml; **Jyske bank,** JBPB, Net Bank user agreement, (EN)-2007, available at: http://www.jyskebank.ch/files/netbank/JBS-NetbankUse Agreement-EN.pdf; **Bank of internet USA**, Privacy Policy, January 2006, available at: http://www.bankofinternet. com/privacy-policy.aspx

(1) **Identity Theft,** Article available at http://www.tqnyc.org/NYC040539/idtheft.html

فورا حتى يقوم البنك باتخاذ كل الإجراءات اللازمة لإيقاف هذا التعدي.

٢٩٠- والسؤال: ما مدى مسؤولية العميل في مواجهة البنك في حالة سرقة البيانات الخاصة بهذا العميل؟

ذهب أحد نماذج العقود الخاصة بالبنوك العاملة على شبكة الإنترنت في سبيل تقرير المسؤولية عن أية مبالغ تفقد بسبب سرقة البيانات الخاصة بالعميل إلى التفرقة بين أمرين[١]:

الأول: إذا ثبت إهمال العميل في اتباع التعليمات التي أوصى بها البنك في المحافظة على هذه البيانات وكيفية استعمالها، حيث حمل العميل كامل المسؤولية في هذه الحالة.

الثاني: إذا ثبت تنفيذ العميل لتعليمات البنك في المحافظة على هذه البيانات وكيفية استعمالها، حيث يتحمل البنك المسؤولية في هذه الحالة.

ويبدو لنا توازن توزيع المسؤوليات بين البنك وعميله في هذا العقد، فالبنك تنتفي مسؤوليته مادام أنه زود العميل بكافة التعليمات والإرشادات الخاصة بالمحافظة على بياناته الشخصية وكيفية استعمالها، ولكن العميل أهمل في اتباع هذه التعليمات؛ كما لو أخبر شخص آخر بهذه البيانات، أو ترك هذه البيانات على جهاز الكمبيوتر الخاص به دون أن يؤمن الدخول إليه، فعليه تحمل تبعات ذلك. أما إذا ثبت التزام العميل بهذه التعليمات، فإن البنك يتحمل المسؤولية عن فقدان

---

(1) **Jyske bank,** JBPB, Net Bank user agreement, (EN)-2007, available at: http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf

هذه المبالغ، سواء كان الأمر يتعلق بخطأ البنك؛ كما لو ثبت للعميل سرقة هـذه البيانات وقام على الفور بإبلاغ البنك بذلك، وقبل البنك على الـرغم مـن هـذا التعامل معه بهذه البيانات، أو كان هناك عطل في أجهزة البنك على النحو الذي سمح بالاطلاع على بيانات العميل أثناء قيامه بإدخالها من قبل الغير، أم لم يثبت خطأ البنك؛ وذلك بموجب قواعد تحمل التبعة (نظرية المخاطر)، وذلك في ضوء المركز القوى الذي يحتله البنك في مواجهة العميل، والذي يبرر تحمله للمسؤولية الناتجة عن مخاطر تقديم العمليات المصرفية على شبكة الإنترنت، حتى ولو لـم يثبت خطأ البنك في مواجهة العميل.

يضاف إلى ما سبق أن الصيغة التي جاءت في هذا العقد(1) تفيد إلقاء عبء إثبات إهمال العميل على البنك. وحسنا ما قرره ذلك العقد، فالبنك فـي مركـز أقوى من العميل بما يملك من أجهزة وبرامج تسيطر على مجريات التعامل بينه وبين عميله، الأمر الذي يجعل من المنطقي إلقاء عبء إثبات هذا الإهمال عليه، ويملك العميل في المقابل أن يثبت مراعاته لهذه التعليمات لدفع مسئوليته.

لكن أيا ما كان شخص المسئول (البنك/العميل)، فإن ذلك لا ينفـي وجـود اعتداء على هذه البيانات.

---

(1) (where the Bank is able to document that You (or someone to whom you disclosed your password and/or key card number/keys) have by gross negligence made unauthorized use possible)
Jyske bank, JBPB, Net Bank user agreement, (EN)-2007, available at:
http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf

٧- مسؤولية سارق البيانات في مواجهة البنك الإلكتروني والعميل:

٢٩١- تتميز سرقة البيانات الشخصية للعميل بتعدد مظاهر الاعتداء المرتكبة، وتعدد الضحايا من جراء هذا الاعتداء، حيث يبدأ بانتهاك أمن البنك الإلكتروني من خلال التوصل إلى هذه البيانات من على قاعدة البيانات الخاصة بالبنك، على أن يلي ذلك الاعتداء على العميل بصورة مباشرة، من خلال انتحال شخصيته والتعامل مع البنك على هذا الأساس بصورة مباشرة أو غير مباشرة(١).

أيضا يمكن أن يبدأ الاعتداء على العميل أولا، وذلك إذا تم الحصول على هذه البيانات وهى في حيازته كما لو كانت مسجلة على جهاز الكمبيوتر الخاص به، أو إحدى الدعامات الإلكترونية الأخرى (مثل بطاقة الائتمان) أو حتى من أحد الملفات الورقية التي يحتفظ بها، على أن يلي ذلك التحايل على البنك الإلكتروني من خلال استغلال هذه البيانات في التعامل بها معه على أنه صاحبها الحقيقي.

وعلى ذلك يحتاج الأمر أن نعرض لمسئولية المعتدى في مواجهة كل من البنك الإلكتروني والعميل، وذلك على النحو التالي:

أولا- مسئولية السارق في مواجهة البنك الإلكتروني:

٢٩٢- تعد سرقة البيانات الشخصية لعميل البنك الإلكتروني نشاطا غير مشروع يقع من قبل المعتدى في حق البنك الإلكتروني على نحو يثير مسئوليته الجنائية

---

(١) د.عبد الله حسين محمود، مرجع سابق، ص٩٦.

Marie Wright; Op. Cit, p. 13.

والمدنية عن هذا الفعل، وذلك على النحو التالي:

أ- المسئولية الجنائية للسارق فى مواجهة البنك:

٢٩٣- يسأل المعتدى جنائيا عن جريمة السرقة في مواجهة البنك الإلكتروني في حالة توصله إلى هذه البيانات من خلال الاستيلاء على الأجهزة أو الدعامات المادية الأخرى التي تحتوي على قاعدة البيانات الخاصة بالبنك، حيث إن هذه الأجهزة منقولات مملوكة للغير تم الاستيلاء عليها بنية تملكها.

وبناءً عليه يخضع المعتدى في هذه الحالة لنص المادة ٣١١ من قانون العقوبات المصري، والتي تنص على "كل من اختلس مالا منقولا مملوكا للغير فهو سارق".

لكن الملاحظ على هذا النص أنه يربط وقوع جريمة السرقة بتحقق الحيازة، الأمر الذي يدعو للتساؤل عن إمكانية وقوع الجريمة في حالة إذا ما اقتصر الأمر على مجرد الاطلاع على هذه البيانات من على أجهزة البنك، أو عبر الموقع الإلكتروني للبنك على الإنترنت.

على الرغم من أن معظم التشريعات العقابية وأحكام القضاء ترفض القول بإمكانية وقوع جريمة السرقة إلا بتحقق الاستيلاء (أي بإخراج الشيء من حيازة صاحبه)، وأن يرد هذا الاستيلاء على شيء مادي- وذلك بسبب ربط هذه الجريمة بالاعتداء على الحيازة- إلا أن قانون العقوبات الانجليزي (الفصل الثالث- الفقرة الأولى، سنة ١٩٦٨) تبنى مفهوما مختلفا لجريمة السرقة، حيث نظر إليها على أنها تشكل اعتداءً على الملكية وليست الحيازة[١]. وبناء عليه

(١) د. شيماء عبد الغنى محمد عطا الله، مرجع السابق، ص٥٣.

ذهب جانب من الفقه[1] إلى تصور وقوع السرقة بمجرد قيام الفاعل بفعل يدل على إدعائه لملكية المعلومات، وذلك كما لو قام بالاطلاع عليها مع علمه بسريتها.

أيضا ما أقرته محكمة النقض الفرنسية في هذا الخصوص، من تقرير وقوع جريمة السرقة لمجرد الظهور على الشيء بمظهر المالك، حتى ولو لم يتحقق الاستيلاء، بإخراج الشيء من حيازة مالكه. فقد أدانت هذه المحكمة شخصا كان يعمل في شركة ما ثم فصل منها، ثم قام بالدخول إلى مقر هذه الشركة وقام بتصوير بعض المستندات الخاصة بها، حيث اعتبرته سارقا للبيانات الموجودة في هذه المستندات لظهوره عليها بمظهر المالك[2].

ونحن من جانبنا نؤيد هذا الموقف، ونرى إمكانية تصور وقوع السرقة حتى ولو لم يتم إخراج الشيء من حيازة مالكه. فمن العناصر الأساسية في فكرة الملكية عنصر الاستئثار، والذي يعطى للمالك الحق في الانفراد باستعمال الشيء والانتفاع به دون غيره، أو السماح للغير بالانتفاع به في حدود معينة يستقل بتقديرها.

ولا شك أن قيام المعتدى بالاستيلاء على البيانات الخاصة بالعملاء من على قاعدة البيانات الخاصة بالبنك يشكل اعتداءً على حق البنك في الاستئثار بهذه البيانات، خاصة إذا كان البنك قد اتخذ كافة الوسائل اللازمة للحفاظ على هذه البيانات، ومنع الاطلاع عليها إلا لأشخاص معينين، وبضوابط محدد. ومن ثم

---

(١) د.**عبد الله حسين محمود**، مرجع سابق، ص ١٧١؛ د. **إسماعيل شاهين**، مرجع سابق، ص ١٥.

(٢) راجع د.**أحمد السيد لبيب**، مرجع سابق، ص ٢١٦

فإن اختراق المعتدى لكل هذه الحواجز والموانع إلى أن يصل إلى الاطلاع على هذه البيانات يتحقق به الاعتداء على حق الاستئثار المقرر للبنك الإلكتروني على هذه البيانات بما يمكن معه للبنك الإلكتروني الرجوع على المعتدى بأحكام جريمة السرقة.

ويسرى ما سبق ذكره على العاملين لدى البنك، وذلك في حالة قيام أحدهم بالتعدى على بيانات أحد العملاء.

والسؤال: هل قيام المعتدى بعد حصوله على البيانات الخاصة بعميل البنك الإلكتروني بالتعامل مع البنك الإلكتروني على أنه الصاحب الحقيقي لهذه البيانات يمكن أن يجعله مسئولا عن جريمة النصب؟

كما سبق أن ذكرنا[1]، من المتصور وقوع جريمة النصب باستخدام وسائل الإلكترونية في مواجهة أجهزة إلكترونية، ومن ثم يسأل المعتدى في مواجهة البنك عن جريمة النصب إذا استعان بالبيانات الخاصة بعميل البنك، وقام بالتعامل معه على أنه الصاحب الحقيقي لهذه البيانات.

ب- المسئولية المدنية للسارق في مواجهة البنك الإلكتروني:

٢٩٤- يسأل المعتدى مدنيا في مواجهة البنك الإلكتروني وذلك بموجب قواعد المسئولية التقصيرية التي ينظمها القانون المدني المصري، والتي تقرر "أن كل خطأ سبب ضررا للغير يلزم مرتكبه بالتعويض"

ويجب على المحكمة عند تقديرها لمبلغ التعويض أن تراعى الأضرار

---

(١) انظر سابقا، ص ٤٢٤.

المادية والأدبية التي لحقت بالبنك من جراء هذه الاعتداءات، علـى أن يـشمل الخسارة التي لحقت بأجهزة وبرامج البنك نتيجة هذا التعدي، وأيـضا الخـسارة التي لحقته في سمعته، وما ترتب على هذه الاعتداءات من زعزعة الثقـة فـي البنك وتعاملاته. كما يجب أن يقدر التعويض في ضوء ما أصاب البنـك مـن خسارة وما فاته من مكسب جراء هذه الأفعال، وذلك وفقا للقواعد العامـة فـي القانون المدني(١).

ثانيا: مسئولية السارق في مواجهة العميل:

٢٩٥- يمكن أن تقع سرقة البيانات الشخصية لعميل البنك الإلكتروني من قبـل المعتدى في حق عميل البنك الإلكتروني أيضا، على نحو يثير مسئوليته الجنائية، والمدنية عن هذا الفعل في مواجهة هذا العميل على النحو التالي:

أ- المسئولية الجنائية للسارق فى مواجهة العميل:

٢٩٦- يسأل المعتدى جنائيا في مواجهة عميل البنك الإلكتروني عـن جريمـة السرقة في حالة توصله إلى البيانات الخاصة بالعميل عن طريق الاستيلاء على الأجهزة المسجل عليها هذه البيانـات (كمبيـوتر الشخـصي، محفظـة النقـود الإلكترونية، بطاقة الائتمان)، أيضا يسأل عن جريمة السرقة في حالـة توصلـه لهذه البيانات من خلال اختراق أجهزة العميل الشخصية والاطلاع عليهـا عبـر شبكة الإنترنت وفقا للأحكام السابق ذكرها في خصوص مسئوليته في مواجهـة البنك الإلكتروني.

أما في حالة قيام المعتدى باستعمال البيانات الخاصة بالعميل والتعامل بهـا

---

(١) انظر المادة ٢٤١ من القانون المدني المصري.

على أنه العميل، فأنه يكون بذلك قد أرتكب جريمة انتحال الشخصية التي تجرمها وتعاقب عليها التشريعات العقابية المختلفة، ومن ثم نحيل في شأن أحكام هذه الجريمة للمراجع العامة في قانون العقوبات.

وفي حالة وقوع أي من الجرائم السابقة من قبل أحد العاملين لدى البنك الإلكتروني في حق أحد العملاء، وذلك من خلال قيامه بالاستيلاء على البيانات الخاصة بالعميل أثناء تعامله مع البنك، والتعامل بهذه البيانات على أنه العميل. فأنه يسأل جنائيا في مواجهة العميل عن جريمة السرقة، وانتحال الشخصية وفق للقواعد سابقة الذكر (في حالة وقوع هذه الجريمة في حق البنك الإلكتروني).

يضاف إلى ذلك، أن العاملين لدى البنك الإلكتروني يقع عليهم عبء الالتزام بالمحافظة على سرية البيانات الخاصة بالتعاملات المصرفية التي تتم بين البنك وعملائه بمناسبة قيامهم بعملهم لدى البنك، وذلك بموجب نص المادة ١٠٠ من القانون رقم ٨٨ لسنة ٢٠٠٣ الخاص بالبنك المركزي والجهاز المصرفي والتي تنص على أن "يحظر على رؤساء وأعضاء مجلس إدارة البنوك ومديريها أو العاملين بها إعطاء أو كشف أية معلومات أو بيانات عن عملاء البنوك أو حساباتهم أو ودائعهم أو الأمانات أو الخزائن الخاصة بهم أو معاملاتهم في شأنها أو تمكين الغير من الاطلاع عليها في غير الحالات المرخص بها بمقتضى هذا القانون".

ويتضح من صياغة هذا النص أنها استعملت كلمة "العاملين بها" بصياغة عامة. تفيد امتداد الالتزام بالسرية إلى كل العاملين لدى البنك الإلكتروني سواء كانوا مصرفيين أو غير مصرفيين. وبناء عليه يسأل العاملين لدى البنك الإلكتروني في حالة اعتدائهم على البيانات الخاصة بعملاء البنك عن جريمة

إفشاء السر المصرفي. هذا وقد نصت المادة ١٢٤ من القانون رقم ٨٨ لسنة ٢٠٠٣ بإصدار قانون البنك المركزي والجهاز المصرفي والنقد على أن "يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز خمسين ألف جنيه كل من خالف أيا من أحكام المادتين ٩٧، ١٠٠ من هذا القانون".

وكما سبق أن ذكرنا[١]، مقدمي الخدمات الإلكترونية للبنك على شبكة الإنترنت (مصمم موقع البنك، ومتعهد الايواء) مخاطبون بأحكام المحافظة على السرية المصرفية، حيث أنهم يطلعون على هذه البيانات بحكم عملهم ووظيفتهم على نحو يجعلهم في حكم العاملين لدى البنك الإلكتروني. وهذا ما نصت المادة السابقة عليه أيضا، حيث قضت بأن "يسرى هذا الحظر على كل من يطلع بحكم مهنته أو وظيفته أو عمله بطريق مباشر أو غير مباشر على البيانات أو المعلومات المشار إليها"[٢]. من ناحية أخرى البنك الإلكتروني غالبا ما يحرص

(١) راجع سابقا، ص ١٧٢.

(٢) وقد تضمن قانون العقوبات الفرنسي نصا جرم من خلاله إفشاء أسرار المهنة، حيث نص في المادة ٢٢٦-١٣ عقوبات على أن " الكشف عن معلومات لها طابع السرية من جانب شخص أمين عليها، سواء بحكم مركزه القانوني أو بحكم مهنته أو بحكم وظيفته. أو مهمة مؤقتة عهد بها إليه، يعاقب بالحبس، وبغرامة لا تتجاوز ١٠٠ يورو"، كما نص أيضا في المادة رقم ٥٧ من القانون الخاص بنشاط مؤسسات الائتمان والرقابة عليها (رقم ٤٦ لسنة ١٩٨٤) على أن "كل عضو مجلس إدارة، أو مجلس للرقابة بحسب الأحوال، وكل شخص يساهم بأي صفة كانت في إدارة أو توجيه مؤسسة مالية أو مستخدم فيها يلتزم بسر المهنة بالشروط ووفقا للعقوبات المنصوص عليها في المواد ٢٢٦ -١٣ و٢٢٦-١٤ من قانون العقوبات". انظر مزيدا من التفصيل **د. غنام محمد غنام**، حدود المسئولية الجنائية للمصارف المالية عن مخالفة واجب السرية وعن غسيل الأموال، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ ه ١٠-١٢ مايو ٢٠٠٣ دبي، ص١٣٢٠ وما بعدها.

في العقود التي تربطه بمقدمي الخدمات الإلكترونية على النص على التزامهم بالمحافظة على سرية البيانات التي يطلعون عليها بحكم عملهم.

وعلى الرغم من استيعاب القواعد العامة في قانون العقوبات المصري لصور الاعتداءات السابقة، إلا أننا كنا نود أن يفرد المشرع المصري نصوصا خاصة لهذه الاعتداءات، وذلك على النحو الذي يراعى فيه الطبيعة الخاصة للمعاملات المصرفية، وما تحتاج إليه هذه المعاملات من معاملة عقابية متميزة خاصة إذا ما كانت تتم عبر شبكة إلكترونية للاتصالات مفتوحة على العالم بأسره كشبكة الإنترنت.

ومما لاشك فيه أن البنوك ومعاملاتها المصرفية هي عصب الاقتصاد القومي في أي مجتمع، بل أن هذه المكانة تزداد إذا كان الأمر يتعلق ببنوك تقدم خدماتها بصورة إلكترونية للعالم بأسره، الأمر الذي يحتاج إلى معاملة عقابية خاصة، تتبنى صيغة عقابية مشددة، توفر من خلالها بيئة قانونية أمنة لهذه البنوك، حتى تحقق أغراضها.

ب- المسؤولية المدنية للسارق فى مواجهة العميل:

٢٩٧- يسأل المعتدى في مواجهة عميل البنك الإلكتروني عن رد كافة المبالغ التي استولى عليها من خلال تعامله بالبيانات الخاصة بهذا العميل. كذلك يلتزم بتعويض العميل عن كافة الأضرار التي لحقت به من جراء انتحال شخصيته، واستعماله غير المشروع لأمواله، وذلك وفقا للقواعد العامة في المسئولية المدنية.

لكن هل يمكن أن يسأل البنك الإلكتروني مدنيا في مواجهة العميل عن سرقة البيانات الخاصة به؟

-المسؤولية المدنية للبنك عن سرقة بيانات عملائه:

٢٩٨- في الواقع يمكن أن تثور المسئولية المدنية للبنك الإلكتروني في مواجهة عميله عن سرقة بيانات الأخير في الحالات التالية:

الأولى: المسؤولية العقدية للبنك. يسأل البنك عقديا في حالة سرقة البيانات الشخصية من على قاعدة البيانات الخاصة بالبنك، يستوي في ذلك وجود نص في العقد الذي ينظم علاقته بالعميل يفيد التزام البنك بتأمين هذه البيانات، أم لا؛ حيث يظل البنك مسئولاً عن ذلك، باعتبار أن تأمين هذه البيانات من الأمور التي تقتضيها طبيعة التعامل المصرفي عبر شبكة الإنترنت، وما تقتضيه قواعد العدالة في هذا الخصوص[١].

ويعد التزام البنك في هذا الصدد التزامًا بتحقيق نتيجة [٢]، فالبنك ملتزم تجاه العميل بتحقيق أمن البيانات الخاصة به والتي يحتفظ بها لديه، وباتخاذ الإجراءات اللازمة لتحقيق هذا التأمين. وبناء عليه إذا حدثت سرقة لبيانات العميل فإنه غير مكلف بإثبات خطأ البنك، حيث إن هذا الخطأ مفترض في حق البنك، ولا يملك

(١) راجع المادة ١٤٨ من القانون المدني المصري والتي تقضي بأن "العقد ملزم لأطرافه ليس فقط في حدود ما ورد به من التزامات، ولكن أيضا بما هو من مستلزماته وفقا لقواعد القانون والعرف والعدالة في ضوء طبيعة الالتزام).

(٢) وأساس النظر إلى التزام البنك الإلكتروني بأنه التزام بتحقيق نتيجة هو تحليل الالتزامات التي ترتبها العقود التي تربط بين البنك وعميله – وفقا للقواعد العامة- نجد أن التزام البنك تجاه عميله يوصف دائما بأنه التزام بتحقيق نتيجة لا ببذل عناية. فمثلا البنك ملزم بتمكين العميل من التعامل مع موقع البنك، والدخول على الحساب الخاص به بسلامة وأمان، وليس فقط بذل العناية لذلك....." انظر د. **شريف محمد غنام**، مسئولية البنك عن أخطاء الكمبيوتر في النقل الإلكتروني للنقود، مرجع سابق، ص٤٨؛

Graham Smith; Op. Cit, p. 278.

الأخير لدفع مسؤوليته في هذه الحالة إلا بإثبات السبب الأجنبي؛ كإثبات أنه اتخذ كافة الإجراءات اللازمة لتأمين موقع البنك وقاعدة البيانات، وأن السرقة تمت بسب عطل مفاجئ في أحد الأجهزة، أو تقصير العميل في اتباع إرشادات الأمن.

الثانية: مسؤولية البنك عن أخطاء العاملين لديه. ويتحقق ذلك في حالة ثبوت وقوع السرقة من قبل أحد العاملين لديه، على أساس مسئولية البنك (بوصفه متبوعًا) عن أخطاء تابعيه؛ فهناك رابطة تبعية بين البنك الإلكتروني والعاملين لديه بحكم عقد العمل بينهم، مادام هذا الخطأ (سرقة البيانات) قد وقع من العامل أثناء تأدية وظيفته أو بسببها. وفي حالة تحقق هذه الشروط تنعقد مسئولية المدنية للبنك الإلكتروني عن خطأ العامل لديه، بحيث لا يستطيع البنك أن يدفع هذه المسئولية بإثبات انتفاء الخطأ من جانبه، أو انعدام علاقة السببية بين الخطأ والضرر، وذلك وفقا للقواعد العامة في القانون المدني المصري.

والتساؤل الذي يطل برأسه علينا، يدور حول مدى إمكانية انعقاد المسؤولية التقصيرية للبنك عن سرقة بيانات العميل.

لا تبدو أهمية لهذا التساؤل إذا ما كان هناك عقد صحيح ينظم العلاقة بين البنك والعميل، حيث يظل الأول مسئولاً عن سرقة هذه البيانات، يستوي وجود نص في العقد يفيد ذلك أم لا. لكن تظهر أهمية هذا التساؤل في حالة عدم وجود عقد بين البنك والعميل، كما لو دخل البنك مع العميل في مفاوضات، على أثرها أدلى العميل ببياناته الخاصة للبنك، ثم فشلت هذه المفاوضات ولم تسفر عن انعقاد العقد أو كان هناك عقد ثم حكم ببطلانه.

في مثل هذه الحالات ووفقا للقانون المصري، لا يمكن الرجوع على البنك تقصيريا إلا في حدود النصوص التي تلزم البنك بالمحافظة على السرية

المصرفية[١]. ولاشك أن هذه النصوص لا تكفى للقول بوجود التزام على البنك بتأمين البيانات الخاصة بالعميل؛ حيث إن مفهوم التأمين وإن كان يشتمل على المحافظة على السرية، إلا أنه ذو مدلول أشمل وأعم منها؛ حيث قد تحدث سرقة للبيانات على الرغم من التزام البنك بالمحافظة على السرية.

ومن خلال مطالعة التشريعات الأخرى، وجد أن القانون الأمريكي الخاص بحماية البيانات (Data Protection Act 1984) قد نظم التزام البنك في هذا الصدد، حيث جعل مسؤولية البنك عن المحافظة على البيانات الخاصة بالعميل ضد كافة أشكال الانتهاكات مسئولية كاملة[٢].

ولعل عبارة مسئولية كاملة توحي بأن البنك مسئوليته مشددة في هذا الخصوص، حيث يكفى أن يثبت العميل تقصير البنك في اتخاذ الإجراءات الأمنية الكفيلة واللازمة لتأمين هذه البيانات (التشفير، وإجراءات التعريف ضد الدخول غير المشروع)، حتى تنعقد مسؤوليته. ولعل هذا التشديد من قبل القانون الأمريكي يجد ما يبرره، وهو حث البنك على اتخاذ كافة الاحتياطات اللازمة للحيلولة دون الاطلاع على البيانات الخاصة بعملائه، على نحو يزيد على ما كان مقرر في نشاط البنوك التقليدية، وذلك بالنظر إلى اتصال البنك بشبكة الإنترنت، وما يحتاج إليه ذلك من بذل البنك قصارى جهده في تأمين بيانات العملاء.

(١) راجع **المادة ٣٧٧** من **قانون التجارة** رقم ١٧ **لسنة ١٩٩٩**، **والمادة ٩٧** من قانون البنك المركزي والجهاز المصرفي والنقد رقم ٨٨ لسنة ٢٠٠٣.

(2) **Graham Smith**; Op. Cit, p. 278.

الفصل الثانى

التوثيق الالكترونى لتأمين البنك على شبكة الانترنت

٢٩٩- عرضنا فيما سبق لبعض صور المخاطر التي يمكن أن يتعرض لها البنك الإلكتروني العامل عبر شبكة الإنترنت، ورأينا كيف أن هذه المخاطر تهدد وجود البنك على هذه الشبكة، الأمر الذي عظم من أهمية الأمن اللازم لتأمين موقع البنك الإلكتروني، وتأمين ما يتم من خلال هذا الموقع من تعاملات مصرفية عبر شبكة الإنترنت.

ولتحقيق هذا الهدف، فقد استلزم الأمر وجود جهات تقدم خدمات أمنية عبر شبكة الإنترنت من أجل تأمين المواقع الإلكترونية ضد مختلف أشكال الهجمات، وتعمل على تعقب المواقع التي تعرض لمنتجات أو خدمات غير مشروعة أو غير آمنة، وتنبه المتعاملين إلى عدم مصداقية هذه المواقع وخطورة التعامل معها، وذلك من خلال إرسال رسائل تحذيرية للمتعاملين بعدم مشروعية هذه المواقع. وتعمل أيضا هذه الجهات على تأمين التعاملات التي تتم عبر هذه المواقع من خلال القيام بدور الوسيط بين الأطراف المتعاقدة والتأكد من هويتهم وأهليتهم القانونية للقيام بالمعاملات، والتأكد من أن الوثائق المتبادلة لم تعدل ولم تغير أثناء إرسالها، كما تقوم بإصدار المفاتيح الإلكترونية التي يمكن بها تشفير المبادلات الإلكترونية وفك هذا التشفير، وإصدار شهادات تصديق تفيد صحة التصرف ونسبته إلى من صدر عنه(١).

---

(1) **E-Banking,** Federal financial institutions examination Council; Op. Cit, p. 9; Background report on Electronic Commerce 1998.

وقد تمثلت هذه الجهات في أفراد أو شركات أو جهات مستقلة تعمل على تأمين وتوثيق التعاملات الإلكترونية التي تتم عبر شبكة الإنترنت، سميت بجهات أو سلطات التوثيق (Certification Authority)(١).

وقد كانت هناك دائما رغبة ملحة تقف وراء اللجوء لنظام التوثيق الإلكتروني على تطويره بشكل مستمر، وهي الرغبة في تسهيل استخدام شبكة قبل الأفراد والمؤسسات، وذلك من خلال تهيئة بيئة آمنة وموثوق

Electronic Commerce Task Force, p 30. available at: http://www.apecsec.org.sg

(١) **د. سمير حامد الجمال**، المرجع السابق، ص ٣٢١.

E-Banking; Op. Cit, p. 7; **Marie Wright**; Op. Cit, p. 10; **William Gram**; Op. Cit, p. 5.

ويلعب التوثيق الإلكتروني دورا كبيرا في تأمين المعاملات على شبكة الانترنت، وهذا ما أوضحه منتدى قانون وسياسية الانترنت (LPF) الذي دعا في بروكسل عام ١٩٩٩ مجموعة عمل دولية تضمنت الخبراء من الحكومات المختلفة (أساتذة جامعات، فنيين، العاملين في القطاع الخاص) ممن يهتمون بالتوثيق الإلكتروني، وأبرزوا أهمية هذا الأمر، وقاموا بوضع مجموعة من المبادئ الاسترشادية للمشرعين الوطنين في مختلف دول العالم وتهدف هذه المبادئ إلى الارتقاء بهذه الخدمات من خلال تهيئة المناخ السياسي والقانوني للاستفادة من هذه الخدمات. وقد جاء ضمن هذه المبادئ ضرورة إزالة كافة العوائق القانونية أمام الاعتراف بالتوثيق الإلكتروني ومشروعية الوسائل التي يتم استخدامها في أنشطته المختلفة، وضرورة ترك مساحة واسعة أمام جهة التوثيق ومن يستفيد من خدماتها في التفاوض حول شروط العقد الذي يحكم تقدم هذه الخدمة بحيث يتلاءم العقد مع طبيعة النشاط المراد حمايته، وغيرها من المبادئ التي تنظم تقديم خدمات التوثيق الإلكتروني عبر شبكة الانترنت.

Working group on international consensus principles for electronic authentication, internet law& policy forum,2005, p1, available at:
http://www.ilpf.org/events/intlprin.htm

بها لإجراء الصفقات الإلكترونية عبر هذه الشبكة[١].

وعلى الرغم من أن المشرع المصري قد أصدر قانونا خاصا باستخدام التوقيع الإلكتروني في نظام التوثيق (القانون ١٥ لسنة ٢٠٠٤) [٢]، إلا أنه من خلال مطالعة نصوص هذا القانون يتبين أن الحالة المسيطرة على المشرع في الأساس هي الاعتراف بحجية الكتابة الإلكترونية والتوقيع الإلكتروني في الإثبات أمام القضاء، ولم يتطرق باستفاضة لتنظيم استخدام نظام التوثيق في تأمين المعاملات الإلكترونية، كما فعلت التشريعات الأخرى.

وعلى العكس من ذلك، فقد سعت بعض النظم القانونية إلى توظيف نظام التوثيق الإلكتروني في تأمين المعاملات الإلكترونية بصورة عامة، والمعاملات المصرفية على شبكة الإنترنت بصورة خاصة. وقد ظهر أثر ذلك فيما قامت به لجنة المحافظين في النظام الاحتياطي الفيدرالي في الولايات المتحدة الأمريكية بعد التشاور مع المنظمات المصرفية الفيدرالية بتقديم تقرير إلى الكونجرس الأمريكي يوصي فيه بضرورة إصدار تشريع ينظم استخدام وسائل التوثيق الإلكتروني في عمل البنك الإلكتروني. وعلى أثر ذلك قام الكونجرس الأمريكي بإصدار قانون التوقيع الرقمي والتوثيق الإلكتروني **Digital}**

---

(1) **Validation test begins for Japan's first electronic authentication system,** available at : http://www.nmda.or.jp/nmda/commerce/kousyou-english.html

(٢) راجع القانون ١٥ لسنة ٢٠٠٤ تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، الجريدة الرسمية، **العدد** ١٧ لسنة. تابع (د)، ٢٢ أبريل ٢٠٠٤.

E-Banking; Op. Cit, p. 7; **Marie Wright**; Op. Cit, p. 10; **William Gram**; Op. Cit, p. 5.

Signature and Electronic Authentication Law (SEAL)} فـــي الثاني من فبراير ١٩٩٨. وقد كان من الأغراض التي وقفت وراء إصدار هـــذا القانون[١]:

١- تسهيل مشاركة المؤسسات المالية في بيئة الأعمال الإلكترونية، مـــن أجـــل ازدهار التجارة الإلكترونية، وأعمال البنوك الإلكترونية.

٢- توفير حماية أكبر للعميل، وذلك من خلال تأمين تعاملاته عبر الشبكة.

٣- التوصل إلى صياغة موحدة للنـــصوص التـــي تحكـــم وتـــنظم التوثيـــق الإلكتروني، وذلك لتجنب تأثيرات تنازع التشريعات الداخلية، والتي تـــؤثر بشكل غير مقصود على تطور البنوك الإلكترونية، أو تخاطر بأمنها.

ومن هنا يظهر لنا مدى أهمية التوثيـــق الإلكترونـــي فـــي حيـــاة البنـــوك الإلكترونية العاملة عبر شبكة الإنترنت، هذه الأهمية تفرض علينا أن نعـــرض لماهية التوثيق الإلكتروني في عمل البنك الإلكتروني (مبحث أول)، على أن يلي ذلك عرض لخدمات التوثيق الإلكتروني في مجال عمل البنك الإلكتروني (مبحث ثاني)، والمسئولية القانونية لجهة التوثيق عن تأمين البنك وتعاملاته(مبحث ثالث)، وذلك على النحو التالي:

---

(1) **Digital signature and electronic authentication law (SEAL) of 1998 (Introduced in Senate)**, available at ; http://thomas.loc.gov/cgi-bin/query/z?c105:S.1594.IS

المبحث الأول

ماهية التوثيق الإلكتروني في عمل البنك على شبكة الإنترنت

٣٠٠- تبدو أهمية وضع تعريف محدد للتوثيق الإلكتروني في عمل البنوك الإلكترونية العاملة عبر شبكة الإنترنت في الرغبة للتوصل إلى صياغة واضحة لطبيعة الخدمات الأمنية للتوثيق الإلكتروني وحدودها في عمل هذه البنوك، بما ينعكس على تحديد طبيعة التزامات جهة التوثيق، ومسئوليتها في مواجهة البنك الإلكتروني. لذلك نعرض أولا لتعريف جهات التوثيق الالكتروني، وذلك لنتعرف على الجهات القائمة على تقديم خدمات التوثيق الإلكتروني، ثانيا لتعريف التوثيق الإلكتروني في عمل البنك الإلكتروني.

أولا- تعريف جهات التوثيق الإلكتروني:

٣٠١- تعددت التعريفات التي تناولت توضيح ماهية جهات التوثيق الإلكتروني إلى تعريفات تشريعية، وتعريفات فقهية، وذلك على النحو التالي:

أ) التعريفات التشريعية:

في مصر نظم قانون التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة التكنولوجيا رقم ١٥ لسنة ٢٠٠٤[1]، ولائحته التنفيذية ١٠٩ لسنة ٢٠٠٥[1] نشاط

(١) انظر هذا القانون على العنوان التالي: http://www.isdo.gov.eg/Esignature-law.asp
راجع أيضا الجريدة الرسمية، العدد ١٧ تابع (د)، ٢٢ أبريل سنة ٢٠٠٤.

جهات التوثيق الإلكتروني، والتي أطلق عليها جهات التصديق الإلكتروني. ولم يضع هذا القانون تعريفا محددا لجهات التوثيق،و لكنه ألزم هذه الجهات بضرورة الحصول على ترخيص بممارسة أنشطتها في مجال التوقيع الإلكتروني من قبل هيئة تنمية صناعة تكنولوجيا المعلومات والاتصالات، كما أخضع هذه الجهات في ممارسة عملها لرقابة هذه الهيئة[٢]. وقد اشتملت باقي مواد القانون على أسس إثبات صحة وحجية التوقيع الإلكتروني وشهادات التصديق الإلكتروني إلى جانب ما يجب أن تحدده اللائحة التنفيذية لهذا القانون من معايير فنية وتقنية وتنظيمية.

وقد نظم التوجيه الأوربي رقم (٩٣) لسنة ١٩٩٩ جهات التوثيق الإلكتروني تحت اسم مقدم خدمة التوثيق (Certification Service Provider)، حيث ألزم هذا التوجيه الدول الأعضاء في الاتحاد الأوروبي بالترخيص بقيام جهات خاصة يعهد إليها باعتماد التوقيعات الإلكترونية عن طريق شهادات تصدرها تفيد استيفاء التوقيع الإلكتروني للشروط اللازمة للاعتماد عليه، وارتباطه بالمستند الذي يرد عليه، مع تأمينه ضد أي تعديل أو تغيير في مضمونه. وقد عرف التوجيه الأوربي هذه الجهات بأنها "كل شخص طبيعي أو اعتباري يقوم بتقديم شهادات إلكترونية للجمهور أو يقدم له خدمات مرتبطة بالتوقيعات الإلكترونية"[٣].

---

(١) راجع **الوقائع المصرية**، العدد ١١٥(تابع)، ٢٥ مايو، ٢٠٠٥.

(٢) وقد نظم القانون العديد من الاختصاصات الأخرى لهيئة تنمية صناعة تكنولوجيا المعلومات والاتصالات، من أهمها محاولة حسم المنازعات التي قد تنشأ بين الأطراف المعنية بأنشطة التوقيع الإلكتروني والمعاملات الإلكترونية. راجع القانون سالف الذكر.

راجع أيضا **الجريدة الرسمية**، العدد ١٧ تابع (د)، ٢٢ أبريل سنة ٢٠٠٤.

(٣) د. **إبراهيم الدسوقي أبو الليل**، مرجع السابق، ص١٨٧٠.

وفي الولايات المتحدة الأمريكية تقوم الوكالة الوطنية لتأمين الصفقات (FAST) على تقديم خدمات التوثيق الإلكتروني، وتخضع في تقديم خدماتها للقانون التجاري الموحد (UCC)، والقانون الموحد لنقل وتبادل المعلومات (UCITA)، و(Common Law)(١).

وقد أطلق قانون الصفقات الإلكترونية السنغافوري عليها اسم سلطة التوثيق وعرفها بأنها عبارة عن "الشخص أو المنظمة التي تصدر شهادات التوثيق الإلكتروني"(٢).

وقد نظم القانون التونسي رقم ٨٣ لسنة ٢٠٠٠ المتعلق بالمبادلات والتجارة الإلكترونية في الفصل الثاني منه هذه الجهات تحت أسم "مزود خدمات المصادقة الإلكترونية" حيث عرفها بأنها " كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني"(٣).

---

(1) **William Gram**; Op. Cit, p. 20

(2) **Electronic transactions ACT 1998**, Legal guide to the electronic transactions ACT, part 1.Preliminary

- أطلق ذات التسمية مجلس الاحتياطي الفيدرالي الأمريكي (**Federal Financial Institutions Examination Council**). انظر:

E-Banking, Federal financial institutions examination Council Op. Cit, p. 7.

- وأيضا دليل التوثيق الإلكتروني الياباني (**Certification authority guidelines**) يطلق عليها ذات التسمية. انظر:

Background report on electronic commerce 1998 ; Op. Cit, p. 30

(٣) انظر هذا القانون على العنوان التالي:

وقد أفرد هذا القانون في الفصل الثامن منه أحكاما خاصة بالهيئة المشرفة على جهات التوثيق، وأطلق عليها اسم الوكالة الوطنية للمصادقة الإلكترونية، ونص على أن هذه الوكالة مؤسسة عمومية لا تكتسب الصبغة الإدارية (ليست من أشخاص القانون العام) وتتمتع بالشخصية المعنوية والاستقلال المالي وأخضعها في علاقتها مع الغير للقانون التجاري.

وقد نظم قانون المعاملات والتجارة الإلكترونية رقم (٢) لسنة ٢٠٠٢ لدولة الإمارات أيضا في الفصل الخامس منه الأحكام المتعلقة بالشهادات وخدمات التصديق. وقد جاء في المادة ٢٣ فقرة (١) أنه "لأغراض هذا القانون يعين الرئيس (رئيس منطقة دبي الحرة للتكنولوجيا والتجارة الإلكترونية والإعلام) بقرار يصدره، مراقبا لخدمات التصديق وعلى وجه الخصوص لأغراض ترخيص وتصديق ومراقبة أنشطة مزودي خدمات التصديق والإشراف عليها، وينشر هذا القرار في الجريدة الرسمية)".

ونظم كذلك مشروع قانون المبادلات والتجارة الفلسطيني أحكام المصادقة الإلكترونية، وقد ذكر في المادة (١) من الفصل الأول منه تعريفا لمزود خدمات المصادقة الإلكترونية بأنه "كل شخص طبيعي أو اعتباري ينشيء ويسلم ويتصرف في شهادات المصادقة الإلكترونية ويقدم خدمات أخري ذات علاقة بالتوقيع الإلكتروني"[١].

---

http://www.arablaw.org/Download/Ec-Tunisia.doc

(١) انظر هذا القانون على العنوان التالى:

http://www.pita-palestine.org/PITA%20files/prOposed%20e-commerce%20law.doc

ب) التعريفات الفقهية:

اختلف الفقه[1] على نفسه في تسمية هذه الجهات، فأطلق البعض عليها "سلطة الإشهار" وذهب إلى تعريفها بأنها "هيئة عامة أو خاصة تسعى إلى ملء الحاجة الملحة لوجود طرف ثالث موثوق به، يقدم خدمات أمنية في التجارة الإلكترونية، من خلال إصدار شهادات تثبت صحة حقيقة معينة متعلقة بموضوع التبادل الإلكتروني، لتوثيق هوية الأشخاص المستخدمين للتوقيع الرقمي، وكذلك نسبة المفتاح العام المستخدم إلى صاحبه".

استخدم جانب آخر اصطلاح "مقدم خدمات التصديق" وعرفها بأنها "هيئة أو مؤسسة، عامة أو خاصة تصدر شهادات إلكترونية، تكون بمثابة سجل إلكتروني يؤمن التوقيع الإلكتروني، ويحدد هوية الموقع، ونسبة المفتاح العام إليه". وتعتبر شهادة التصديق بمثابة بطاقة هوية الكترونية تستخرج من شخص مستقل ومحايد ومرخص له بمزاولة هذا النشاط.

وأطلق جانب ثالث على هذه الجهات اصطلاح "مقدم خدمات التصديق الإلكترونى" وذهب في تعريفها بأنها "شخص طبيعي أو معنوي يستخرج الشهادات الإلكترونية، ويقدم الخدمات الأخرى المرتبطة بالتوقيعات الإلكترونية، ويضمن تحديد هوية الأطراف المتعاقدة، والاحتفاظ بالبيانات الخاصة بالشهادة لمدة معينة، ويلتزم باحترام القواعد المنظمة لعمله، والتي يتم تحديدها بمعرفة السلطة المختصة".

والملاحظ على مجموع هذه التعريفات أمران:

---

(١) انظر د. **سمير حامد الجمال**، مرجع السابق، ص٣٢١.

الأول/ أنها ركزت على ضرورة حصول جهة التوثيق على ترخيص بممارسة نشاطها، القوانين التي تخضع لها في ممارسة نشاطها، دون أن تسلط الضوء على طبيعة عمل ونشاط جهات التوثيق.

الثاني/ أنها تناولت تعريف جهات التوثيق بصيغ مختلفة، بل وجاءت تتناول أحد جوانب اختصاصات جهات التوثيق (التوقيع الإلكتروني، شهادات التوثيق)، غافلة عن الاختصاصات الأخرى، كما أن الصيغة المتبعة توحي بقصر اختصاص هذه الجهات على الاختصاصات التي وردت في التعريف، على الرغم من أن هذه الجهات تشهد تطويرًا مستمرًا في نشاطها واتساع دائرة هذه الاختصاصات، على نحو لا يقبل معه وضع اختصاصات محددة في التعريف، حتى لا يصطدم بمعطيات الواقع.

لذلك نرى أن تعرف جهة التوثيق الإلكتروني بأنها عبارة عن شخص طبيعي أو معنوي يرخص له بتقديم خدمات أمنية للمعاملات الإلكترونية على شبكة الإنترنت.

ثانيا- تعريف التوثيق في نظام عمل البنك الإلكتروني:

٣٠٢- يعد أول ظهور للتوثيق الإلكتروني في نظام التجارة الإلكترونية، كان في العمليات المصرفية الإلكترونية[١]، وذلك عندما تم اللجوء إليه للتعرف على

---

(١) ولعل هذا يجد تبريرا له في طبيعة المعاملات المصرفية وما تحتاج إليه من ضرورة التعرف والتأكد من شخصية العميل قبل التعامل المصرفي معه، خاصة إذا ما كان هذا التعامل يتم عن بعد من خلال وسيلة إلكترونية، حيث تدعو الحاجة بشدة إلى تمييز العميل والتحقق منه. د. **على أحمد مرسى عثمان**، مرجع سابق، ص ٤٤؛ وانظر أيضًا:

Thomas C. Glaessner, Tom Kellermann, Valerie Mc Nevin; Op.

شخصية العميل عند استخدامه بطاقات الائتمان، حيث كان يتم الاتفاق فيما بين أطراف التعامل بالبطاقة على أحد أشكال التوثيق للتعرف على شخصية العميل، والتي كان من أشهرها أرقام التعريف الشخصية[١] (PIN)[٢].

وتبدو أهمية وضع تعريف واضح للتوثيق الإلكتروني في نظام عمل البنك العامل عبر شبكة الإنترنت؛ من خلال النظر إلى الدور الذي يلعبه التوثيق في تأمين وجود البنك وتعاملاته عبر شبكة الإنترنت، الأمر الذي يدعو إلى ضرورة توضيح ماهيته من أجل التعرف على نطاقه ووظائفه في نظام عمل البنك، وذلك على النحو التالي:

١) التعريف التشريعي:

لم يظهر لنا تشريع يضع تعريفا للتوثيق الإلكتروني في نظام عمل البنوك العاملة عبر شبكة الإنترنت. ولم يظهر لنا في هذا الخصوص إلا تعريفات للتوثيق الإلكتروني بصورة عامة، الأمر الذي يعكس رغبة التشريعات القانونية في المساواة بين الأمرين.

Cit, p. 71

(1) **Alfred M. Pollard,** Op. Cit, available at: http://www.senate.gov/~banking/97_10hrg/102897/witness/pollard.htm

(٢) ويشير اختصار (PIN) إلى رقم التعريف الشخصي (personal identification number)، وهو عبارة عن رقم مكون من مجموعة من الأعداد يقوم عميل البنك الإلكتروني باختياره عند بداية التعامل، بحيث يعتمد عليه في الدخول إلى الخدمات المصرفية الإلكترونية التي يقدمها البنك، ويعتمد عليه البنك في التحقق من شخصية العميل قبل التعامل معه. وهذه الأرقام شخصية، حيث يجب على العميل أن يحرص دائما على سريتها.

HSBC, Terms and Conditions for Internet Banking; Op. Cit.,

هذا وقد تعددت التشريعات التي تعرضت لتوضيح ماهية التوثيق الإلكتروني بصورة عامة، وإن اختلف مسلك كل منها في ذلك: فمنها من عرفه بصورة مباشرة ومنها من عرفه من خلال سرد لأهم الخدمات التي تقدمها جهات التوثيق. وقد يبرر لهذه التشريعات موقفها هذا (وضع التعريفات) بالرغبة في توضيح وإبراز ماهية التوثيق الإلكتروني، بالنظر إلى حداثة الفكرة، وأهميتها في ذات الوقت. وقد جاءت هذه التعريفات على النحو التالي: .

جاء قانون التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤ يخلو من تعريف للتوثيق الإلكتروني. هذا وقد حاولت هيئة تنمية صناعة تكنولوجيا المعلومات أن تخفف من غلواء هذا الأمر، بأن عرضت لأهم خدمات التوثيق المقدمة من جهة التوثيق في كراسة شروط ومتطلبات منح تراخيص تقديم خدمات التوقيع الإلكتروني لهذه الخدمات، وهي (١):

- إصدار شهادة تصديق الكتروني.
- نتيجة فحص بيانات إنشاء توقيع الكتروني.
- أدوات إنشاء التوقيع الإلكتروني (البطاقة الذكية + القارئ).
- أي أعمال أخري تتعلق بتنظيم التوقيع الإلكتروني.

ويلاحظ على الخدمات السابقة أنها تعكس رؤية ضيقة لمفهوم خدمات

---

(١) انظر كراسة شروط ومتطلبات منح تراخيص تقديم خدمات التوقيع الإلكتروني الصادرة عن هيئة تنمية صناعة تكنولوجيا المعلومات الأحكام العامة، المادة ١٠ فقرة (١)، ص ١٠، متاح على العنوان الإلكتروني التالي:

http://www.itida.gov.eg/csp

التوثيق الإلكتروني؛ حيث قصرتها هيئة تكنولوجيا صحة المعلومات فقط على خدمات التوقيع الإلكتروني، التي هي أحد صور خدمات التوثيق وليست كل الخدمات.

ومن خلال مطالعة موقف التشريعات الأخرى في هذا الخصوص، يتبين أن قانون التوقيع الرقمي والتوثيق الإلكتروني الأمريكي[1]، قد تعرض بصورة مباشرة لتعريف التوثيق الإلكتروني؛ حيث عرفه بأنه "مصطلح يشير إلى التشفير أو الوسائل الإلكترونية الآمنة الأخرى التي تسمح لمستعمل هذه الوسائل بأن:

أ- يتأكد من الهوية[2] أو المعلومات المتعلقة بمن يتم التعامل معه.

ب- التأكد من أن الوثائق المتبادلة بين الأطراف المتعاملة لم تعدل ولم تغير أثناء إرسالها.

ج- التأكد من أن الوثائق المستلمة أرسلت من قبل الطرف المحدد (المرسل).

أيضا تعرضت المادة الثانية من قانون المعاملات والتجارة الإلكترونية لدولة الإمارات رقم (٢) لسنة ٢٠٠٢ [3] لتعريفه بأنه "الإجراءات التي تهدف إلى

---

(1) **Digital signature and electronic authentication law (SEAL) of 1998 (Introduced in Senate)**, available at: http://thomas.loc.gov/cgi-bin/query/z?c105:S.1594.IS:

(٢) مصطلح **الهوية** أوسع نطاقا من مصطلح الاسم، حيث يشمل مصطلح الهوية تمييز الشخص عن غيره من الأشخاص الأخرى بالاسم أو بغيره من وسائل التمييز الأخرى كالمنصب أو الوضع الاجتماعي. انظر **محمد سعيد أحمد إسماعيل**، مرجع السابق، هامش، ص١٩٨.

(٣) هذا القانون متاح على العنوان التالي: http://www.arablaw.org/Download/Ec-UAE.doc

التحقق من أن رسالة إلكترونية قد صدرت من شخص معين، والكشف عن أي خطأ أو تعديل في محتويات أو في نقل أو تخزين رسالة إلكترونية أو سجل إلكتروني خلال فترة زمنية محددة، ويشمل ذلك أي إجراء يستخدم مناهج حسابية أو رموزًا أو كلمات أو أرقامًا تعريفية أو تشفيرًا أو إجراءات للرد أو لإقرار الاستلام وغيرها من وسائل حماية المعلومات".

ويلاحظ على موقف كل من القانون الأمريكي والإماراتي أنهما قد تبنيا رؤية أكثر اتساعا من القانون المصري، حيث عرفا التوثيق الإلكتروني بأنه مجموعة الإجراءات التي تهدف إلى تأمين التبادل الإلكتروني للبيانات، وذلك من خلال التأكد من صدور رسالة البيانات من الشخص الذي له صفة في إصدارها، وأن هذه الرسالة لم تتعرض للتحريف أو التغيير. لكن يبدو لنا أن هذه التعريفات لا تزال قاصرة عن الإحاطة بما يجب أن تكون عليه خدمات التوثيق الإلكتروني من تغطية فكرة أمن البنك العامل عبر شبكة الإنترنت بالمفهوم الذي سبق أن أشرنا إليه[1].

٢) التعريف الفقهى

جاءت التعريفات الفقهية انعكاسا للتعريفات التشريعية، من تبنى نظرات ضيقة لمفهوم التوثيق الإلكتروني.

فقد عرف من قبل جانب من الفقه[2]، بأنه عبارة عن "العملية التي تهدف إلى

(١) راجع سابقا، ص ٥٠٦.

(2) **Authentication & authorization for electronic resources**, article available at : http://www.usc.edu/its/services/authx/

التحقق والتأكد من أن الشخص الذي قدم بياناته هو فعلا صاحب هذه البيانات".

وعرف أيضا بأنه عبارة عن مجموعة الإجراءات التي تهدف إلى التحقق (verify) من شخصية عملاء البنك الإلكتروني الجدد، والتصديق(authenticate) على العملاء الحالين للبنك، وذلك عند الدخول على الخدمات المصرفية الإلكترونية(١).

٣) **رأينا الخاص:**

وعلى الرغم من صحة التعريفات السابقة فيما ذهبت إليه، إلا أنه يبدو لنا أنها لم تعط التوصيف الأمثل لما يجب أن تكون عليه خدمات التوثيق الإلكتروني. فقد تبنت نظرة ضيقة لمفهوم التوثيق الإلكتروني، بأن قصرته فقط على مجرد تأمين التبادل الإلكتروني للبيانات من خلال إصدار شهادات التوثيق وخدمات التوقيع الإلكتروني. وتتمثل أوجه القصور في هذه التعريفات في أمرين:

الأول/ أن مفهوم الأمن على شبكة الإنترنت أكبر من مجرد تأمين التبادل الإلكتروني للبيانات عبر هذه الشبكة، ولكن يحتاج الأمر أيضا إلى تأمين المقدرات الإلكترونية على شبكة الإنترنت (كتأمين المواقع الإلكترونية). فكما سبق أن ذكرنا قد يتحقق الاعتداء على أمن الموقع الإلكتروني من خلال الدخول

---

(1) **Authentication in an electronic banking environment**, August 2001,available at: http://www.cdt.org/privacy/eudirective/EU_Directive_.html

غير المشروع عليه. دون أن يؤثر ذلك على سلامة التبادل الإلكتروني للبيانات بينه وبين المتعاملين معه. لذلك كان يجب أن يأتي التوثيق الإلكتروني بخدماته لتغطية هذا المفهوم الشامل للأمن، وهذا ما لم تحققه التعريفات السابقة.

الثاني/ أن جهة التوثيق ليس هناك ما يمنعها من تقديم كافة خدمات التأمين الإلكتروني على شبكة الإنترنت، لتشمل ليس فقط مجرد تأمين التبادل الإلكتروني للبيانات، ولكن أيضا تأمين المواقع الإلكترونية ضد كافة أشكال الانتهاكات التي تتم عبر الشبكة، خاصة أن تأمين تبادل البيانات مرتبط بتأمين الموقع الذي تتم من خلاله صور التعامل الإلكتروني المختلفة. هذا من ناحية.

ومن ناحية آخري، تقديم خدمات التأمين على وجه الخصوص يتطلب أن يتم عبر جهة موثوق بها، تخضع لرقابة الدولة فيما تمارسه من أنشطة[1]، تلك الرقابة التي تضمن استيفاء هذه الجهات لكافة المعايير التي تؤهلها لتقديم مثل هذه الخدمات من حيث الأجهزة والأدوات التي تعتمد عليها والعاملين الذين تستعين بهم لتقديم خدماتها، الأمر الذي قد لا يتوفر لغيرها من الشركات التي تقدم خدمات التأمين الإلكتروني.

وبناء عليه يبدو لنا ضرورة تبنى مفهوم أكثر اتساعا وشمولية لمفهوم خدمات التوثيق الإلكتروني خاصة تلك التي تقدم للبنك العامل عبر شبكة الإنترنت، فإذا ما ربطنا ما سبق ذكره بطبيعة البنك الإلكتروني العامل عبر شبكة الإنترنت سواء من حيث تصميمه الفني، أم من حيث طبيعة المعاملات التي يقدمها، نلاحظ أنه ليس مجرد موقع يقدم خدمات معلوماتية تحكمها المراسلات الإلكترونية

---

(1) **Kit Burden**; Op. Cit, p. 249

البسيطة، ولكنه موقع تفاعلي مرتبط بشبكة إلكترونية داخلية تدير وتنفذ حركة المعاملات المصرفية عبر هذا الموقع، الأمر الذي يفضل معه تبني منظومة أمنية واحدة على مستوى البنك ككل، تقوم عليها جهة موثوق بها كجهة التوثيق الإلكتروني، تعمل على تزويد البنك بكل ما يحتاج إليه لتأمين موقعه وتعاملاته المصرفية التي تتم عبر هذا الموقع من خلال مجموعة من العاملين الفنيين المؤهلين لذلك، على نحو يحقق أمن البنك على شبكة الإنترنت. يضاف إلى ذلك المخاطر التي تهدد أمن البنك على شبكة الإنترنت، سواء تلك التي تستهدف موقعه الإلكتروني، أم الشبكة الداخلية، الأمر الذي يحتاج إلى خدمات أمنية تتناسب مع حجم وطبيعة هذه المخاطر.

ويدعم موقفنا في هذه النظرة الشمولية لخدمات التوثيق في نظام عمل البنك العامل عبر شبكة الإنترنت، ما يلي:

أ) ما حرصت علي توضيحه جمعية تطوير وسائل الإعلام الجديدة في اليابان (The New Media Development Association)، حيث عملت على تطوير الجزء الخاص بنظم التوثيق الإلكتروني باعتباره جزءًا هامًا من مشروعات تطوير التجارة الإلكترونية، وأن ذلك يتحقق بتأمين المواقع على الشبكة وتأمين الخدمات الإلكترونية التي يتم الحصول عليها من هذه المواقع(١).

ب) أيضا ما ذهبت إليه وزارة الصناعة البريطانية في البيان الصادر عنها، والتي أبرزت من خلاله الدور المحوري لجهات التوثيق الإلكتروني ليس

(1) Validation Test Begins for Japan's first Electronic authentication system, Op, Cit

فقط لتقديم خدمات التوثيق (التوقيع الإلكتروني، شهادات التوثيق)، ولكن في كل ما يشمل تأمين المعاملات الإلكترونية، خاصة ما يتعلق منها بالخدمات المالية(١).

ت) كذلك من خلال النظر إلى تصنيف شهادات التوثيق التي تقوم الوكالة الوطنية للمصادقة الإلكترونية بتونس بإصدارها، حيث يلاحظ أنها تصدر ثلاثة أنواع من الشهادات على النحو التالي(٢):

- شهادة تراسل إلكتروني تمكن من تحديد هوية صاحب الشهادة، والتي ترتبط بعناصر التوقيع الإلكتروني الخاص به.

- شهادة خاصة بتحديد هوية الموقع، تمكن من تحديد هوية صاحب التوقيع، والمصادقة عليه.

- شهادة خاصة بالشبكة، وهي تمكن من تحديد هوية الشبكات الخاصة الافتراضية وتضمن سلامة جميع المبادلات التي تتم عبرها.

ويعكس هذا التصنيف على هذا النحو تأكيد ما ذكرناه، من اتساع مفهوم التوثيق الإلكتروني ليشمل ليس فقط تأمين المعاملات الإلكترونية التي تتم عبر شبكة الإنترنت، ولكن أيضا تأمين المواقع الإلكترونية التي تتم من خلالها هذه المعاملات.

---

(1) **Kit Burden**; Op. Cit, p. 249

(٢) المؤتمر الإقليمي العربي الإفريقي حول سلامة المبادلات والإمضاء الإلكتروني وهيكل المفتاح العمومي، **في نطاق الإعداد لفعاليات القمة العالمية لمجتمع المعلومات تونس ٢٠٠٥، متاح على العنوان التالي:**
http://www.certification.tn/Conference/PKITunisia2005/index.htm

ث) وفي الإطار ذاته ذهب جانب من الفقه[1] إلى القول بأن "دور جهات التوثيق الإلكتروني لا يقتصر على تحديد هوية المتعاملين في التعاملات الإلكترونية، وتحديد أهليتهم القانونية للتعامل والتعاقد، وإنما تقوم بالإضافة إلى ذلك بالتحقق من مضمون هذا التعامل، وسلامته، وجديته، وبعده عن الغش والاحتيال، وأيضا العمل على تعقب المواقع التجارية على الإنترنت للتحري عنها وعن جديتها ومصداقيتها".

ج) أيضا ما أوصى به منتدى قانون وسياسة الإنترنت (LIPF) من ضرورة تبني التشريعات القانونية في الدول المختلفة لمفهوم واسع للتوثيق الإلكتروني بحيث يمتد ليشمل تأمين مختلف المعاملات الإلكترونية على شبكة الإنترنت[2].

لذلك نرى تعريف التوثيق الإلكتروني في مجال عمل البنك الإلكتروني بأنه عبارة عن مجموعة الإجراءات التي تسعى إلى تامين وجود البنك الإلكتروني على شبكة الإنترنت، وتأمين المعاملات المصرفية التي تتم عبر موقعه الإلكتروني.

---

(١) د. إبراهيم الدسوقي أبو الليل، مرجع السابق،ص ١٨٦٩؛ د. خالد ممدوح إبراهيم، مرجع سابق، ص ٧٤.

(2) **Working group on International consensus principles for electronic authentication**; Op .Cit, p. 1.

المبحث الثاني

خدمات والتزامات جهة التوثيق في نظام عمل البنك

٣٠٣- تبدو أهمية التعرض لخدمات التوثيق الإلكتروني في نظام عمل البنك العامل عبر شبكة الإنترنت في نقل صورة عن الجانب التطبيقي لهذه الخدمات في نظام عمل البنك، من أجل تسليط الضوء على طبيعة عمل جهة التوثيق تجاه البنك، وخاصة أن هذه الخدمات حديثة العهد بالنشاط المصرفي، على نحو تدعو معه الحاجة إلى التعرف على طبيعة هذه الخدمات وتناسبها مع طبيعة المخاطر التي تهدد أمن البنك على شبكة الإنترنت. كما أن عرض هذه الخدمات يبرز طبيعة الالتزامات القانونية التي تقع على عاتق جهة التوثيق في مواجهة البنك وعملائه، وطبيعة مسؤوليته القانونية الناشئة عن الإخلال بهذه الالتزامات. كما توضح على صعيد آخر الاحتياطات التي يجب على كل من البنك وعميله الالتزام بها لتأمين التعامل المصرفي بينهم عبر شبكة الإنترنت، لذلك سنعرض لأهم خدمات التوثيق الإلكتروني فى عمل البنك، والتزامات جهة التوثيق بخصوص هذه الخدمات، وذلك على النحو التالى:

المطلب الأول

خدمات التوثيق الالكتروني فى نظام عمل البنك

٣٠٤- وتجدر الإشارة إلى أن هناك تعددًا وتنوعًا في خدمات التوثيق الإلكتروني في مجال المعاملات الإلكترونية على شبكة الإنترنت بصورة عامة. وإزاء ذلك نلاحظ أن هذه الخدمات تختلف من مؤسسة لأخرى بحسب طبيعة

الخدمات التي تقدمها كل مؤسسة، وبحسب حجم نشاطها.

وعكس ذلك، فإن مقدم خدمات التوثيق للبنك الإلكتروني يجب أن يراعى تناسب الخدمات الأمنية كما وكيفا مع حجم نشاط البنك، وخصوصية الخدمات المصرفية التي يقدمها[١]. فمثلا يجب أن يراعى تعاظم أهمية السرية والخصوصية في المعاملات المصرفية، وذلك مقارنة بغيرها من المعاملات، كما يجب أن يراعى في ذات الوقت ما تحتاج إليه الخدمات المصرفية من سهولة وبساطة في حصول العميل عليها، وذلك على النحو الذي يجب ألا تتسم فيه إجراءات التأمين بالصعوبة والتعقيد. هذا من ناحية.

ومن ناحية أخرى، يجب مراعاة حجم تعاملات البنك على شبكة الإنترنت، حيث إن الأمر يختلف من بنك لأخر، في ضوء طبيعة الخدمات المصرفية التي يقدمها، الأمر الذي يفرض مراعاة حجم تعاملات البنك، حتى تأتى خدمات التأمين متناسبة مع ذلك.

وبناء عليه، فإن إنجاز طرق مناسبة وملاءمة للتوثيق الإلكتروني للبنك تبدأ بضرورة تقدير طبيعة وحجم الاعتداءات التي يمكن أن يتعرض لها أثناء عمله على شبكة الإنترنت، وتقييم هذه الاعتداءات في ضوء نوعية الخدمات المصرفية التي سيقدمها البنك وحجمها، ومن ثم تقديم البرامج الأمنية المناسبة التي تتلاءم مع هذه المخاطر. كذلك يجب مراعاة مدى خطورة وحساسية البيانات المخزنة في أنظمة عمل البنك الإلكتروني المختلفة[٢].

---

(1) **G C Chalikias;** Op, Cit, p. 59

(2) **Authentication in an electronic banking environment**; Op. Cit, p. 8.

ولتوضيح الفكرة، فإن الأمر يحتاج لعرض أهم خدمات التوثيق التي تتلاءم وطبيعة عمل البنك على شبكة الإنترنت، كما يلي :

أولا- وسائل التحقق من شخصية عميل البنك الإلكتروني :Authentication mechanisms

٣٠٥- تقتضي طبيعة التعامل عبر شبكة للاتصال الإلكتروني عن بعد من ناحية، والأهمية الخاصة للبنك في التعرف على شخصية المتعامل معه من ناحية أخرى، اعتماد البنك على مجموعة من وسائل التحقق والتأكد من شخصية العميل تلائم طبيعة المعاملات المصرفية على شبكة الإنترنت. ولاشك في أهمية هذه الوسائل في تحصين البنك الإلكتروني ضد العديد من أشكال الانتهاكات التي تستهدف أمنه، خاصة انتهاكات الدخول غير المشروع على أنظمة البنك. وتتميز هذه الوسائل بالتعدد والتنوع، وذلك على النحو الذي يتيح الفرصة أمام البنك لتنويع الاستفادة من هذه الوسائل بما يتلاءم مع طبيعة وحجم المعاملات المصرفية، وبما يتلاءم مع ظروف وطبائع العملاء.

ومن أهم الوسائل المستخدمة لتحقق البنك من شخصية عميله: التوقيع الإلكتروني وشهادة التوثيق الإلكتروني وكلمة المرور[١]. ومهما كانت قوة وفاعلية الوسائل السابقة من الناحية الفنية، إلا أنها لا تؤتي ثمارها المرجوة إلا في ظل تنظيم قانوني يحكم استخدامها في علاقة البنك بالعميل، وذلك على النحو التالي:

---

(1) E-Banking; Op, Cit. p. 7.

(١) التوقيع الإلكتروني:

٣٠٦- يقتضى الحديث عن التوقيع الإلكتروني كوسيلة لتأمين المعاملات المصرفية عبر شبكة الإنترنت، إبراز أهمية هذا التوقيع، والتعرف على ماهيته، وذلك على النحو التالي:

أ) أهمية التوقيع الإلكتروني في تأمين المعاملات المصرفية عبر شبكة الإنترنت:

٣٠٧- يلعب التوقيع الإلكتروني(١) دورا كبيرا في مجال تحديد هوية عملاء البنك العامل عبر شبكة الإنترنت، وإثبات صحة التصرفات الصادرة عنهم في مواجهة البنك، والتأكد من أن البيانات التي تصل إلى البنك هي البيانات التي أرسلوها بالفعل، ولم يتم العبث بها من قبل أي شخص(٢).

وقد تعرض قانون التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤ لهذه الأهمية، وذلك عندما تعرض في المادة ١٨ لدور التوقيع الإلكتروني في التأكد من هوية المتعامل، ونسبة التصرف إليه؛ حيث جاء في هذه المادة أنه "يتمتع التوقيع الإلكتروني بالحجية في الإثبات إذا ما توافرت الشروط التالية:

---

(١) يقصد بكلمة إلكتروني في مفهوم التوقيع الإلكتروني وفقا للمادة الأولى من قانون البحرين الخاص بالمعاملات والتجارة الإلكترونية الصادر في ١٤ سبتمبر ٢٠٠٢ " تقنية استعمال وسائل كهربائية أو مغناطيسية أو كهرومغناطيسية أو بصرية أو بايومترية أو فوتونية أو أي شكل آخر من وسائل التقنية المشابهة". هذا القانون متاح على الموقع التالي: http://www.arab-elaw.com/show_similar.aspx?id=71

(2) **E-Banking** Federal financial institutions examination council; Op. Cit,p7;**Background report on electronic commerce 1998**; Op. Cit, p. 30. **Graham Smith**; Op. Cit, p. 278.

- ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.
- سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.
- إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

وعلى الرغم من أن صياغة المشرع المصري توحي بإبراز دور التوقيع الإلكتروني في الإثبات، إلا أنه عرض بصورة غير مباشرة لدور التوقيع الإلكتروني في تأمين التبادل الإلكتروني للبيانات من خلال عرضه للشروط التي يجب أن تتوافر في هذا التوقيع للاعتراف به.

أيضا بيّن التوجيه الأوربي الخاص بالتوقيع الإلكتروني[1]، أهمية هذا التوقيع

---

(1) **Directive 1999/93/EC** (on Electronic Signatures), Official Journal of the European Communities, article 2 (2)

- هذا وقد عنيت العديد والعديد من التشريعات بتنظيم أحكام التوقيع الإلكتروني نظرا لأهميته الكبيرة في تأمين المعاملات في التجارة الإلكترونية، ومن أهم هذه التشريعات:

- القانون النموذجي للتجارة الإلكترونية الصادر عام ١٩٩٦ (UNCITRAL Model Law on Electronic Commerce 1996)، وذلك في المادة (٧) فقرة أولى.
- قانون الصفقات الإلكترونية السنغافوري الصادر عام ١٩٩٨ (Singapore Electronic Transactions Act 1998).
- قانون التوقيع الإلكتروني الأسباني الصادر عام ١٩٩٩ (Spain's Electronic Signatures).
- قانون الاتصالات الإلكترونية البريطاني (UK Electronic Communications Act 2000).
- القانون النموذجي للتوقيع الإلكتروني ٢٠٠١ (UNCITRAL Model Law on Electronic Signatures 2001).

في المادة الثانية فقرة (٢) وذلك من خلال ذكر أهم الخصائص التي يتميز بها التوقيع الإلكتروني والتي تعكس في ذات الوقت أهم وظائفه، وهي:

- أنه مرتبط فقط بشخص الموقع.
- يمكن من خلاله التحقق من شخصية الموقع.
- أن هذا التوقيع ينشأ بأدوات تتواجد فقط تحت سيطرة الموقع.
- أنه مرتبط برسالة البيانات الموقعة على النحو الذي يترتب على تعديل هذا التوقيع تغيير في محتوى الرسالة.

أيضا تعامل قانون التوقيع الإلكتروني في الولايات المتحدة الأمريكية، مع التوقيع الإلكتروني باعتباره من أهم الوسائل المستخدمة في تأمين معاملات التجارة الإلكترونية[١].

وقد نظم القانون الفرنسي رقم (٢٣٠ ــ ٢٠٠٠) في شأن المبادلات والتجارة الإلكترونية هذا الأمر، فقد ورد ضمن أحكام هذا القانون أن التوقيع الإلكتروني يدل على شخصية الموقع، ويضمن علاقته بالواقعة المنسوبة إليه إلى أن يثبت العكس[٢].

ولعل كثرة التشريعات القانونية التي تناولت التوقيع الإلكتروني بالتنظيم أمر

---

http://www.smaldonado.com/marcos/docs/ct_esig_su_eu_en.html
Kit Burden; Op. Cit, p. 248.

(1) **E-Banking,** federal financial institutions examination council; Op. Cit, p. 7.

(٢) د. **عبد الفتاح بيومى حجازى**،مرجع السابق، ص١٧. وما بعدها.

ينم عن أهميته الكبرى في تأمين المعاملات الإلكترونية بصورة عامة، والتي يأتي في مقدمتها المعاملات المصرفية، الأمر الذي يدعو إلى ضرورة التعرض لتعريف هذا التوقيع وصوره وذلك في ضوء طبيعة النشاط المصرفي للبنك العامل عبر شبكة الإنترنت.

ب) تعريف التوقيع الإلكتروني:

٣٠٨- تعددت التعريفات التي تعرضت للتوقيع الإلكتروني، والتي عكست وجهات نظر متعددة لتصور هذا التوقيع ووظائفه، وذلك على النحو التالي:

- التعريف التشريعي:

عرف قانون التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤ في المادة الأولى منه التوقيع الإلكتروني بأنه "ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون لها طابع منفرد يسمح بتحديد شخص الموقع وتمييزه عن غيره".

وتعرض لتعريفه أيضا قانون الأونيسترال النموذجي للتوقيع الإلكتروني لسنة ٢٠٠١[(١)]، حيث عرفه بأنه عبارة عن "بيانات إلكترونية مدرجة أو مضافة أو مرتبطة منطقيا برسالة بيانات[(٢)] تستخدم لتعيين هوية الموقع على المعلومات

---

(1) **UNCITRAL Model law on electronic signatures**; Op. Cit, p. 1. available at:

- وهذا هو ذات التعريف الذي تبناه مشروع قانون التجارة الإلكترونية الانجليزي.

Kit Burden; Op. Cit, p. 248.

(٢) وتعرف **برسالة البيانات** وفقا **للمادة الثانية من هذا القانون** بأنها عبارة عن "**معلومات** يتم إنشاؤها أو إرسالها أو استلامها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة. بما في ذلك (على سبيل المثال) التبادل الإلكتروني **للبيانات** أو البريد الإلكتروني أو

الواردة في هذه الرسالة، وبيان موافقة الموقع على ما ورد فيها من بيانات".

وعرفه التوجيه الأوربي سالف الذكر[١] بأنه عبارة عن "بيانات في شكل إلكتروني تندرج أو ترتبط بشكل منطقي مع بيانات إلكترونية أخرى وتعمل كوسيلة للتوثيق".

وعرفه أيضا قانون البحرين الخاص بالمعاملات والتجارة الإلكترونية في المادة الأولى منه على "أنه معلومات في شكل إلكتروني تلحق بسجل إلكتروني أو تثبت أو تقترن به منطقيا ويمكن للموقع استعمالها لإثبات هويته".

- **التعريف الفقهي:**

عرف جانب من الفقه[٢] التوقيع الإلكتروني بأنه عبارة عن "كل إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع ومرتبطة ارتباطا وثيقا بالتصرف القانوني، وتسمح بتمييز شخص صاحبها وتحديد هويته، وتنم، دون غموض عن رضائه بهذا التصرف القانوني".

عرفه جانب آخر[٣] بأنه عبارة عن "مجموعة حروف أو أرقام أو رموز أو أصوات إلكترونية أو تشفير رقمي أو أي نظام معالجة إلكترونية آخر، بحيث يمكن أن يميز ويحدد هوية شخص موقعه، وبحيث يمكن ارتباطه بمضمون المحرر الثابت على أية دعامة إلكترونية".

البرق أو التلكس أو النسخ البرقي".

(1) **Directive** 1999/93/EC, Official Journal of the European Communities, article 2 (1).

(٢) **د. ثروت عبد الحميد**، التوقيع الإلكتروني، دار النيل للطباعة والنشر، ٢٠٠١، ص٤٩.

(٣) **د. سمير حامد الجمال**، مرجع سابق، ص ٢١٦.

والملاحظ على جميع هذه التعريفات أنها ركزت على إظهار أهم وظائف التوقيع الإلكتروني وهي التعرف على هوية الموقع وتمييزه عن غيره، ونسبة التصرف الذي يحمل توقيعه إليه من الناحية القانونية. ولا يختلف مفهوم التوقيع الإلكتروني في نظام عمل البنك الإلكتروني عن المفاهيم السابقة.

لذلك يبدو لنا أن نعرف التوقيع الإلكتروني في مجال عمل البنوك العاملة عبر شبكة الإنترنت بأنه عبارة عن مجموعة بيانات إلكترونية ذات طابع مميز تسمح بتحديد شخصية العميل ونسبة التصرف إليه من الناحية القانونية عند التعامل مع البنك عبر شبكة الإنترنت.

ولاشك في أهمية التوقيع الإلكتروني بهذا المعنى في العلاقة بين البنك وعميله، حيث يزيد الحرص لدى البنك دون غيره من المؤسسات العاملة عبر شبكة الإنترنت في التعرف والتحقق من شخصية العميل؛ نظرا للطبيعة المالية للمعاملات المصرفية، الأمر الذي يزيد من أهمية التوقيع الإلكتروني بالنسبة للبنك في التحقق والتأكد من شخصية العميل بخصوص كافة المراسلات الإلكترونية خاصة طلبات الحصول على الخدمات المصرفية.

ت) صور التوقيع الإلكتروني في نظام عمل البنك الإلكتروني:

٣٠٩- تتعدد صور وتطبيقات التوقيع الإلكتروني في نظام البنك العامل عبر شبكة الإنترنت[1] ولاشك في أهمية هذا الأمر؛ حيث يزيد من فرص استفادة البنك منه في مختلف العمليات المصرفية. لذلك تبدو أهمية التعرف على نظام عمل كل صورة من هذه الصور، كي نبرز مزايا وعيوب كل صورة ومدى

(١) د. ثروت **عبد الحميد**، مرجع سابق، ص ٤٩.

إمكانية الاستفادة منها في نظام عمل البنك. أيضا يلتزم البنك بإعلام العميل بكافة التفاصيل الفنية لعمل هذه التوقيعات، الأمر الذي يزيد من الحاجة إلى التعرف على نظام عمل كل صورة من هذه الصور، وذلك على النحو التالي:

(١) التوقيع البيومترى Biometric Signature[١]:

٣١٠- تتمتع هذه الصورة من صور التوقيع بدرجة عالية من الثقة. ويعود هذا إلى اعتماد هذا النوع من أنواع التواقيع الإلكترونية على حقيقة علمية ثابتة مفادها أن لكل أنسان صفات ذاتية خاصة به لا توجد لدى غيره، وتتميز بالثبات النسبي، مما يزيد من الثقة في هذا التوقيع، وأنه قد صدر من الموقع فعلا[٢].

ويعرف هذا التوقيع بأنه عبارة عن أسلوب من أساليب التحقق من الشخصية بالاعتماد على الخواص الفيزيائية والطبيعية والسلوكية للأشخاص مثل: بصمات الأصابع ونبرة الصوت وقزحية العين[٣].

ومن الناحية التطبيقية، يتم العمل بالتوقيع البيومترى من خلال تجهيز نظم

---

(١) وتعنى كلمة البيومترية (Biometrics) القياسات الحيوية. وهي تطلق على الوسائل المرتبطة مباشرة بالصفات المميزة والخواص الفيزيائية والطبيعية والسلوكية للانسان، والتي تختلف من شخص لآخر. وقد شهدت الأنظمة البيومترية هذه تطورا عام ١٩٩٨، وذلك عندما بدأت شركة (OKI) اليابانية للصناعات الكهربائية، ومؤسسة (Citibank) الأمريكية في نيويورك باختبار لبعض الأنظمة التي تعتمد على قزحية العين لاستعمالها في جهاز الصرف الآلي للنقود، حيث تقوم هذه التجربة على تثبيت كاميرا رقمية تعمل على مطابقة الخواص البشرية التي تقوم بالتقاطها مع تلك الخواص المخزنة فيها، وذلك للتأكد من شخصية العميل. انظر **محمد سعيد أحمد إسماعيل**، مرجع السابق، ص١٩٣.

(٢) **إيمان مأمون سليمان**، مرجع السابق، ص٢٥٦.

(3) G C **Chalikias**, Op. Cit, p. 64.

انظر أيضا: د. **عبد الفتاح بيومي حجازي**، المرجع السابق، هامش ص ٣٤.

المعلومات الخاصة بالبنك الإلكتروني بحيث تسمح بتخزين الصفات والخواص الطبيعية والسلوكية الخاصة بالعملاء بطريقة مشفرة، ثم يتم التقاط صورة دقيقة لصفة جسدية لعميل البنك الإلكتروني عند تعامله مع البنك، كعينه أو صوته أو يد أو بصمته الشخصية، ثم يتم مطابقتها بما هو مخزن على أجهزة البنك، والتي يتم برمجتها على أساس عدم السماح بالتعامل إلا بعد مطابقة هذه البصمة مع البصمة المبرمجة في ذاكرته، ومن ثم لن يتم التعامل إلا مع الأشخاص المصرح لهم بذلك(١).

ومن أهم النواحي الايجابية في استخدام التوقيع البيومترى ما يلي(٢):

- أنه لا يعتمد على المفاتيح السرية وما يتعلق بها من مشاكل خاصة تتعلق بنسيان أو تزوير أو سرقة أرقام وكلمات السر.
- يعتمد على خواص طبيعية خاصة تختلف من عميل لآخر، ولا يمكن القول بوجود فردين متماثلين في هذه الخواص.

لكن مع ذلك وجهت سهام النقد لاستعمال التوقيع البيومترى، حيث ذهب البعض إلى القول بأن هذه الوسيلة تتسم بالضعف- على الرغم من التصريحات المعلنة من الجهات المختصة بتقديم خدمات التوقيع البيومترى من ارتفاع درجة الأمان لهذا النوع من التوقيع- لكون هذه الوسيلة يتم الاحتفاظ بها في ذاكرة أجهزة الحاسب مما يجعلها عرضة للهجوم والنسخ من قبل المعتدين أو محاولة تقليد ومحاكاة هذه الخواص البشرية؛ حيث يمكن تقليد بصمات الأصابع باستخدام

(1) **G C Chalikias;** Op, Cit, p. 58.

(٢) **محمد سعيد أحمد إسماعيل**، المرجع السابق، ص١٩٣.

بصمات بلاستيكية مقلدة، أو استخدام أنواع معينة من العدسات اللاصقة بنفس اللون والشكل والخصائص، كما يمكن تسجيل بصمة الصوت وإعادة بثها؛ ومن ثم فهي وسيلة تفتقر إلى الأمان والسرية، وخاصة أن الجهات المنتجة للوسائل البيومترية تعمل على توحيد نظم عملها، كما أنها لا تقدم نتائج كاملة الصحة(١).

ونرى أن كل أوجه النقد السالفة، والتي حاولت النيل من التوقيع البيومترى لا تؤثر فيما يتمتع به هذا النوع من أنواع التواقيع من درجة عالية من الثقة والأمان في التعريف بشخصية العميل؛ وذلك للأساس الذي تقوم عليه هذه الوسيلة للتعريف بشخصية صاحبها، ألا وهى خصائص وصفات أعضائه البشرية التي لا تتوافر لدى أحد غيره بذات الشكل والمواصفات. أما ما سبق ذكره من إنتقادات فهى أمور يمكن التغلب عليها من خلال توفير تقنيات لتشفير هذا التوقيع لحمايته ضد التعرف عليها أو محاولة تقليده، من خلال توفير نظم تكنولوجية تحقق ذلك.

(٢) التوقيع بالقلم الإلكتروني:

٣١١- يعتمد هذا النوع من التوقيع على قيام عميل البنك الإلكتروني باستخدام قلم إلكتروني حساس، يمكنه الكتابة على شاشة الحاسب الآلي على أن يكون هذا الحاسب مزود ببرنامج معلوماتي يعمل على إتمام عملية التوقيع الإلكتروني من خلال مرحلتين :

الأولى: التقاط التوقيع:

يتم في هذه المرحلة تلقى بيانات العميل عن طريق بطاقة تحقيق الهوية

---

(١) د. **سمير حامد الجمال**، مرجع السابق، ص٢٢٥.

الإلكترونية الخاصة به، ثم تظهر بعد ذلك على الشاشة رسالة تطلب من العميل كتابة توقيعه باستخدام القلم الالكتروني داخل مربع ظاهر على الشاشة. يقوم البرنامج بعد ذلك بالتقاط حركة يد العميل أثناء تحريك يده وكتابة التوقيع، ويظهر هذا التوقيع مكتوبا على الشاشة بكل سماته وخصائصه، من حيث الحجم وشكل الحروف والمنحنيات والخطوط والدوائر، بالإضافة إلى السرعة النسبية التي يتم بها وضع الحروف. يظهر للعميل بعد ذلك ثلاثة أيقونات: الأولى للموافقة على شكل التوقيع، الثانية لإعادة المحاولة الثالثة لإلغاء التوقيع. فإذا وافق العميل على شكل التوقيع الذي ظهر أمامه فإنه يقوم بالضغط على أيقونة موافق، حيث يقوم البرنامج بتجميع هذه البيانات وتشفيرها(١).

الثانية: التحقق من صحة التوقيع:

يقوم البرنامج في هذه المرحلة بفك الشفرة وإجراء المطابقة بين البيانات التي تم إدخالها من قبل العميل، والبيانات المخزنة لديه، حيث يعطى هذا البرنامج إشارة، تظهر على جهاز العميل بما يفيد مطابقة التوقيع من عدمه(٢).

وقد تميزت هذه الطريقة من طرق التوثيق بسهولة الاستخدام؛ حيث يقوم العميل بكتابة توقيعه التقليدى (الذى يقوم بكتابته على المحررات الورقية) لكن على شاشة الكمبيوتر، حيث يقوم البرنامج بمعالجة هذه البيانات على نحو يجعلها ملائمة للتعامل بها في البيئة الإلكترونية(٣). يضاف إلى ذلك صعوبة تزوير هذا التوقيع، حيث إن البرنامج يعمل على التأكد من صحة هذا التوقيع الذي يكتبه

---

(١) المرجع السابق، ص٢٢٦.

(٢) **محمد سعيد أحمد إسماعيل**، مرجع سابق، ص ١٩٧.

(٣) **د. سمير حامد الجمال**، مرجع سابق، ص٢٢٦.

العميل من خلال إجراء المطابقة بين التوقيع الذي يكتبه العميل وبين التوقيع المحفوظ لديه بدقة كبيرة يسهل معها اكتشاف أي تزوير[١].

ولم تمنع هذه المزايا من توجيه سهام النقد لهذا النوع من أنواع التواقيع، والتي تركزت في ضعف الثقة والأمان؛ واللذين يعودان إلى احتمالية إساءة استخدام التوقيع من قبل المرسل إليه، الذي يستطيع أن يحتفظ بنسخة من هذا التوقيع ثم يقوم بوضعه على أي مستند آخر ليس صادرًا عن صاحب التوقيع، ومن ثم هذا من شأنه أن يعدم الصلة بين التوقيع والمحرر الذي يحمله[٢].

لكننا نرى أنه لا مجال للقول بإساءة استخدام التوقيع من قبل المرسل إليه في ظل وجود جهة التوثيق، والتي تعمل على تشفير هذا التوقيع ومراقبة استخدامه على نحو يتوفر له الثقة والأمان في الاستعمال. يضاف إلى ذلك أن هناك تقنيات لا تسمح بإعادة نسخ البيانات الإلكترونية، أو إعادة استخدامها، ومن ثم يمكن أن نستفيد من تقنية التوقيع بالقلم الإلكتروني كوسيلة للتعريف بشخصية العملاء عند التعامل مع البنك الإلكتروني، مع مراعاة احتياطات الأمان اللازمة.

(٣) التوقيع الرقمي:

٣١٢- يعد التوقيع الرقمي من أكثر الطرق التي يمكن أن يلجأ إليها البنك الإلكتروني للتعرف على شخصية العميل؛ وذلك نظرا لما يقوم به هذا التوقيع من قوة الربط بين الموقع والتصرف الصادر عنه[٣]. هذا بالإضافة إلى سهولة

---

(١) إيمان مأمون سليمان، مرجع سابق، ص٢٥٩.

(٢) د. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، المرجع السابق، ص ٢٠٠.

(3) **Graham Smith**; Op. Cit, p. 278.

استخدام هذا التوقيع[١]. ويسمى هذا التوقيع بالفرنسية signature numerique ويسمى بالإنجليزية digital signature.

وقد كانت بداية استخدام التوقيع الرقمي في المعاملات المصرفية الإلكترونية، حيث كانت البطاقات الذكية Smart card وبطاقات الموندكس Mondex card والتي تحتوى على رقم سرى تطبيقا عمليا لهذا التوقيع من خلال التعامل مع جهاز الصرف الآلي ATM حيث كان الرقم السري الموجود في هذه البطاقات وسيلة للتعريف بشخصية العميل، ثم تطور استخدام هذا التوقيع وبدأ يستخدم في الرسائل المتبادلة إلكترونيا[٢].

وقد تعددت تعريفات هذا التوقيع، فقد ذهب البعض[٣] في تعريفه بأنه عبارة عن "أرقام مطبوعة (تسمى Hash) على محتوى المعاملة التي يتم التوقيع عليها بالطريقة ذاتها، أي باستخدام الأرقام" في حين ذهب جانب آخر[٤] إلى القول بأنه عبارة عن "بيانات أو معلومات متصلة بمنظومة بيانات أخرى أو صياغة منظومة في صورة شفرة".

وذهب جانب ثالث[٥] للقول بأنه عبارة عن "توقيع ينشأ بعلاقة رياضية ذات صفة فريدة من الناحية الاحتمالية، ويرتبط بالبيانات المخزنة على شكل إلكتروني

---

(1) **Kit Burden**; Op. Cit, p. 248; **A. Michael Froomkin**, ; Op. Cit, p. 5.

(٢) د. **خالد ممدوح إبراهيم**، المرجع السابق، ص١٩٨.

(٣) د. **إبراهيم الدسوقى أبو الليل**، مرجع ابق، ص١٨٥٦.

(٤) د. **خالد ممدوح إبراهيم**، المرجع السابق، ص١٩٨.

(٥) **محمد سعيد أحمد إسماعيل**، المرجع السابق، ص١٩٨.

للقيام بالوظائف المختلفة للتوقيع".

ولنا ملاحظتان على التعريفات السابقة:

الأولى: أنها تعرضت لوصف التوقيع دون أن تتعرض لذكر وظائفه.

الثانية: أن هذه التعريفات تقترب من التعريفات الخاصة بالتوقيع الإلكتروني، وهذا أمر طبيعي حيث إن التوقيع الرقمي ما هو إلا صورة من صور التوقيع الإلكتروني.

لذلك نرى أن يعرف التوقيع الرقمي بأنه عبارة عن شكل من أشكال التوقيعات الإلكترونية، والتي تستخدم في التعرف على شخصية الموقع، والتأكد من صدور التصرف عنه، وذلك من خلال استخدام مفاتيح سرية تعمل على تحويل بيانات التوقيع من صورته المفهومة والمقروءة إلى صورة غير مفهومة ولا مقروءة، على أن يتم إعادته لصورته الأصلية من قبل الشخص المخول له بذلك.

وينشأ التوقيع الرقمي ويتم التأكد من صحته باستخدام التشفير[1]، أي من

---

(١) يجب ألا نخلط بين أمرين: تشفير التوقيع، وتشفير الرسالة. فإذا كان كل منهما عملية رياضية تهدف إلى تغيير المحتوى المراد تشفيره على نحو يحفظ عليه سريته، إلا أنهما يختلفان في أن تشفير الرسالة يشملها بالكامل بما في ذلك التوقيع، في حين أن تشفير التوقيع فقط يقتصر على التوقيع فقط دون مضمون الرسالة، وعلى ذلك يمكن أن نتصور توقيعًا مشفرًا ورسالة إلكترونية غير مشفرة. انظر: **إيمان مأمون سليمان**، مرجع السابق، ص٢٧١.

- وقد اعترف المشرع التونسي بالتشفير كوسيلة لنقل البيانات حيث جاء في **الفصل الثالث من القانون رقم ٨٣ لسنة ٢٠٠٠ بشأن المبادلات والتجارة الإلكترونية** "يخضع استعمال التشفير في المبادلات والتجارة الإلكترونية عبر الشبكات العمومية للاتصالات إلى الترتيب الجاري بها العمل في ميدان الخدمات ذات القيمة المضافة

خلال تحويل صيغة التوقيع من صورته المقروءة والمفهومة إلى صورة غير مفهومة وغير مقروءة. فمثلاً لو أراد عميل البنك الإلكتروني إرسال رسالة بيانات عبر البريد الإلكتروني للبنك، فإنه يقوم بإعداد ملخص لهذه الرسالة باستخدام برنامج التشفير وباستخدام المفتاح الخاص، ثم يقوم بإرسالها للبنك. وحتى يتأكد البنك من صحة مصدر الرسالة وأنها صدرت عن العميل فإنه يقوم باستخدام المفتاح العام المرتبط بالمفتاح الخاص للعميل لفك شفرة الرسالة، ثم يقوم البنك بعد ذلك بإعداد ملخص للرسالة باستخدام نفس برنامج التشفير، ويقارن بين ملخص الرسالتين، فإذا كانتا متطابقتين فأن هذا يدل على أن الرسالة صحيحة ولم يطرأ عليها أي تعديل أو تحريف، ومن ثم التأكد من وصول الرسالة من العميل فعلا. أما إذا لم يقم المفتاح العام للبنك بفك شفرة الرسالة، أو كان هناك اختلاف بين ملخص الرسالتين فإن هذا يدل على أن الرسالة لم تصل من العميل(1).

ومن أهم ما يتميز به التوقيع الرقمي كوسيلة لتأمين معاملات البنك الإلكتروني العامل عبر شبكة الإنترنت أن أي تغيير يطرأ على الرسالة الموقعة يؤدى إلى تغيير في التوقيع المرتبط بها مباشرة، مما يساعد على اكتشاف حدوث

للاتصالات" .

(1) **Kit Burden,** Op. Cit, p. 248.

- وقد أثيرت هذه المسألة في إحدى المنازعات التي عرضت على القضاء الانجليزي **(Standard Bank London Ltd v Bank of Tokyo Ltd)**، والتي تتلخص في تمكن أحد المخادعين من إعادة إرسال ذات الرسائل التي سبق أن أرسلها البنك للعميل والتي تحمل التوقيع الإلكتروني الخاص بالبنك، حيث قضت المحكمة بمسؤولية العميل عن إهماله في فحص الرسالة والتأكد من مطابقة التوقيع الرقمي للبنك.

Graham Smith; Op. Cit. p. 278.

التغيير[١].

ويتميز التوقيع الرقمي كوسيلة يمكن أن يعتمد عليها البنك الإلكتروني للتعرف على شخصية العميل بالعديد من المزايا أهمها[٢]:

- يؤدى إلى التحقق من هوية العميل، وأن الرسالة الموقعة منه تنسب إليه، فلا يمكن له إنكار الرسالة. ويعود ذلك إلى الارتباط التام بين المفتاح العام والخاص.
- يحقق التوقيع الرقمي- بفضل تقنيات التشفير التي يعتمد عليها- سرية المعلومات التي يتضمنها المحررات الإلكترونية، حيث لن يتمكن من الاطلاع على الرسالة إلا البنك الإلكتروني الذي يمسك بالمفتاح العام.
- يعبر بطريقة واضحة عن إرادة العميل للالتزام بالتصرف القانوني الصادر عنه، وقبوله لمضمونه، ومن ثم يحقق كافة الشروط التي يتطلبها القانون في المحرر كي يصلح لأن يكون دليلا كتابيا كاملاً في الإثبات.

ولاشك في مزايا استخدام التوقيع الرقمي للتعريف بشخصية عميل البنك الإلكتروني لكن هذه المزايا لا تتحقق ما لم يتم استخدام هذا التوقيع تحت إشراف جهة التوثيق، والتي تلعب دورا كبيرا في عمل هذا التوقيع. ويظهر ذلك في

---

(1) **A. Michael Froomkin**; Op. Cit, p. 6.

(٢) **إيمان مأمون سليمان**، مرجع السابق، ص٢٦٩.

A. Michael Froomkin; Op. Cit, p. 6.

Jyske bank, JBPB, Net Bank user agreement, (EN)-2007, available at:

http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf

توفير تقنيات التشفير التي يقوم عليها عمل التوقيع الرقمي، وكذلك العمل على توثيق هذا التوقيع من خلال شهادات التوثيق الإلكترونية التي تقوم بإصدارها بعد أن يقوم عميل البنك الإلكتروني باتباع إجراءات التسجيل الخاصة بهذا التوقيع لدى جهة التوثيق(١).

هذا وقد صاغ المشرع المصري في قانون التوقيع الإلكتروني ١٥ لسنة ٢٠٠٤ (٢)شروطا للاعتداد بالتوقيع الرقمي كوسيلة لإثبات نسبة التصرف لصاحبه، وهي:

أ) ارتباط التوقيع بالموقع وحده دون غيره.

ب) سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.

ج) إمكانية كشف أي تعديل أو تغيير في بيانات المحرر الإلكتروني.

أيضا نص قانون الصفقات الإلكترونية السنغافوري(٣) أنه يشترط في التوقيع الرقمي كوسيلة لتأمين المعاملات الإلكترونية:

- أن يتم استعمال التوقيع الإلكتروني خلال الفترة التي تكون فيها شهادة التوثيق(التي يرتبط بها التوقيع الرقمي) سارية المفعول، وصحيحة ومرتبطة بالمفتاح العام المدرج فيها

- أن تكون شهادة التوثيق قد صدرت بمراعاة اعتبارات الثقة والأمان من قبل

---

(1) **Background report on electronic commerce** 1998; Op. Cit, p. 30.

(٢) هذا القانون متاح على العنوان الإلكتروني التالي:

http://www.isdo.gov.eg/Esignature-law.asp

(3) **Electronic transactions ACT 1998**, Op. Cit, part VI (Effect of digital Signatures).

جهة مرخص لها بإصدار الشهادات وتراعى أحكام القانون.

- أن تكون الأطراف المتعاملة (البنك الإلكتروني والعميل) قد اتفقت بينها بشكل صريح على استخدام التوقيع الرقمي كوسيلة لتامين المعاملات فيما بينهم.

وبعد العرض لصور التوقيع الإلكتروني المختلفة والمتعددة يتبين لنا أمران:

الأول: تعدد وتنوع هذه الوسائل من شأنه أن يجعل فرصة الاختيار أمام القائمين على تشغيل البنك الإلكتروني كبيرة، حيث يمكنهم استخدام كل هذه الوسائل أو اختيار ما يتناسب فقط مع الإمكانيات المتاحة. يضاف إلى ذلك إمكانية توظيف هذه الوسائل في استخدامات مختلفة، كتأمين موقع البنك على شبكة الإنترنت، أو تأمين الملفات الموجودة داخل أجهزة البنك، أو تأمين المراسلات المتبادلة بين البنك والعميل. كل ذلك من شأنه أن ينعكس على حسن إدارة وتشغيل البنك[١].

الثاني: أن تزويد البنك الإلكتروني بمثل هذه الوسائل من شأنه أن يوفر درجات عالية من الأمن الإلكتروني أثناء عمل البنك على شبكة الإنترنت، مما يعزز من ثقة المتعاملين مع البنك في قدرة البنك في العمل، وتقديم الخدمات على شبكة الإنترنت بأمان.

ث) ارتباط عمل التوقيع الإلكتروني بشهادة التوثيق:

ويعتمد نظام العمل بالتوقيع الإلكتروني بمفهومه السابق، وبصوره المختلفة،

---

(1) **E-Banking,** Federal financial institutions examination Council; Op. Cit, p. 7; **Background report on electronic commerce 1998**; Op. Cit, p. 32.

على حصول حامل التوقيع على شهادة توثيق من جهة مرخص لها قانونا بإصدار هذه الشهادات، حيث تفيد هذه الشهادات في ربط التوقيع بشخصية الموقع.

وتلعب شهادة التوثيق الإلكتروني بهذا المعنى دورا كبيرا في التعامل مع البنك الإلكتروني عبر شبكة الإنترنت؛ الأمر الذي يحتاج إلى التعرف على طبيعة التنظيم القانوني لهذه الشهادة، وهذا ما سنوضحه في موضع تال[١]، باعتبار أن إصدار شهادة التوثيق هو من أهم الالتزامات الواقعة على عاتق جهة التوثيق.

(٢) كلمة المرور Password:

٣١٣- تعد كلمة المرور من أكثر الطرق التي يعتمد عليها البنك الإلكتروني للتحقق من شخصية العميل[٢]، وذلك لما تتمتع به هذه التقنية من قبول عام (popular acceptance)، يعود إلى ما تتميز به هذه التقنية من سهولة في الاستعمال من قبل العملاء من ناحية، وأنها ذات قدرة على التكيف مع أنظمة العمل المختلفة على موقع البنك الإلكتروني من ناحية أخري؛ حيث يمكن الاعتماد عليها للتحقق من شخصية العميل عند دخوله على موقع البنك، أو عند قيامه بطلب إحدى الخدمات المصرفية التي يقدمها البنك، أو غيرها من نظم

---

(١) انظر لاحقا، ص ٦٧٢.

(2) **James E Backhouse**, Security: The Achilles heel of electronic commerce; Op. Cit, p. 30; **Bank of Internet USA**, Website Agreement, available at:
http://www.bankofinternet.com/website-usage-legal-policy.aspx

العمل الأخرى[1].

وتعرف كلمة المرور بأنها عبارة عن شكل من أشكال التحقق السري من شخصية العميل، وذلك بهدف التحكم في عملية الدخول للبنك عبر شبكة الإنترنت، والتي تحفظ بعيدا عن الاطلاع من قبل الأشخاص غير المسموح لهم بالتعامل مع البنك الإلكتروني[2].

---

(1) **M. Sklira. A. S. pomportsis. M. S. Obaidat**, A framework for the design of bank communications, Op, Cit, p.1780.

(2) **Password**, From Wikipedia, the free encyelopedia, available at: http://en.wikipedia.org/wiki/Password

consumer rights in electronic fund transfers, California department of consumer affairs division of legal affairs(Legal Guide CR-6): Op, Cit., p. 2.

- وتعتمد فعالية كلمة المرور من الناحية الفنية كوسيلة لتأمين المعاملات الإلكترونية مع البنك الإلكتروني على طول وتركيبة كلمة المرور password Length and Composition. وتقاس قوة وفعالية كلمة المرور بطولها وتركيبتها. ويعتمد تحديد الطول والتركيبة المناسبة لكلمة المرور على مدى قيمة وحساسية المعلومات المراد حمايتها بواسطة كلمة المرور. فكلما كانت المعلومات المراد حمايتها تمييز بالحساسية والدقة، كلما كان ذلك دافعا لاختيار تركيبات أكثر تعقيدا لكلمة المرور. واختيار كلمة المرور من قبل عميل البنك الإلكتروني يحتاج منه إلى الاعتماد على معايير معينة وتتمثل هذه المعايير في:

أ - الجمع بين الأرقام والرموز عند اختيار كلمة المرور.

ب- ومراعاة وجود تفاوت واختلاف في هذا الترتيب الأبجدي للحروف المستخدمة في تكوين هذه الكلمة. ومراعاة مثل هذه المعايير في اختيار كلمة المرور أمر ضروري بسبب أن المحاولات لمعرفة كلمة المرور تسعى إلى ذلك من خلال إنتاج ملايين المجموعات من الحروف الأبجدية، وذلك من أجل تخمين أكبر قدر ممكن من كلمات المرور التي يحتمل استخدام العميل لها.

Thomas C. Glaessner, Tom Kellermann, Valerie McNevin, Electronic safety and Soundness; Op, Cit, p. 127; **Authentication in an electronic banking environment**. Op. Cit, p. 8.

٣١٤- التنظيم القانوني لاستخدام كلمة المرور في علاقة البنك بالعميل:

يفرض استخدام كلمة المرور التزام كل من العميل والبنك بمراعاة أمور معينة لضمان سلامة وأمن استخدام كلمة المرور، وذلك على النحو التالي:

أ- بالنسبة للعميل:

تعتمد سلامة كلمة المرور على قدرة العميل على المحافظة على سرية (password secrecy) هذه الكلمة ضد أي محاولة للتعرف عليها من قبل الغير[1]. وتتعدد الطرق التي يمكن من خلالها انتهاك سرية كلمة المرور الخاصة بعميل البنك الإلكتروني، ومن أشهر هذه الطرق:

- التقاط كلمة المرور أثناء استخدامها من قبل العميل. وتتمثل هذه الطريقة في قيام المعتدى بمراقبة السلوكيات التقنية لصاحب كلمة المرور (User behavior techniques) أثناء تعاملاته المختلفة على شبكة الإنترنت، حتى ولو كانت المعاملة مع غير البنك، حيث قد يلجأ العميل إلى استخدام كلمة مرور واحدة لعدة استخدامات على شبكة الإنترنت، الأمر الذي يأخذه المعتدى في اعتباره عند تخمين هذه الكلمة.

- اقتحام الملفات الخاصة بكلمة المرور، والتي قد يحتفظ بها العميل على الكمبيوتر الخاص به، والذي لا يراعى تأمين الدخول على هذا الكمبيوتر.

لذلك يلتزم العميل دائما بتوخي الحذر الشديد عند تعامله مع المواقع المختلفة

(1) Tips for **Safe Banking over the Internet**, Op. Cit, p. 1.

عبر شبكة الإنترنت، وعدم الدخول على مواقع غير موثقة أو غير معتمدة[(١)]. كذلك يلتزم بأن يحيط كلمة المرور والملفات التي تتضمنها بنظم تشفير قوية لحماية سرية هذه الكلمات[(٢)].

ويجب أن يحرص البنك على تنظيم هذه الالتزامات في التعاقدات التي تحكم تعامل العميل معه، وأن يحمله المسؤولية عن الإخلال بهذه الالتزامات[(٣)].

ب- بالنسبة للبنك الإلكتروني:

يلتزم البنك الإلكتروني باتباع أسلوب منظم للتحكم في تشغيل كلمة المرور password system controls [(٤)] الخاصة بعملائه، وتتمثل مظاهر هذا التحكم فيما يلي[(٥)]:

- مراقبة مدى طول كلمة المرور التي يقوم العملاء باستعمالها، ومتطلبات تركيبها، وأن يكون لديه القدرة على تغير هذا التركيب

---

(1) **Graham Smith**; Op. Cit, p. 278.

(2) **Tips for Safe Banking Over the Internet**, Op. Cit,. p. 1; **S.K Leong, T. Srikanthan, G. S. Hura**, Op. Cit, p. 3.

(٣) راجع نماذج للعقود المصرفية التي تنظم التزام العميل في هذا الشأن على المواقع الإلكتروني التالية:

http://www.germanbanks.org/shOp/index.asp#verbraucherrecht

www.deutsche-bank-pbc.pl/content/pdf/en/Internet_wniosek_umowa_ang.pdf

https://www.firmenfinanzportal.de/fb/en/pdf/agb_GeschaeftsbedigungenFernkommunikation_en. pdf

(4) **Graham Smith**; Op. Cit, p. 278.

(5) **Authentication in an electronic banking environment**, Op. Cit, p. 7.

تدعو إلى ذلك.

- السيطرة على كل طرق الدخول للبنك الإلكتروني والخروج منه عبر شبكة الإنترنت.

- مراعاة انتهاء صلاحية كلمة المرور وحالات إلغائها في حالة حدوث أي انتهاك لسريتها.

- مراعاة متطلبات التوثيق الخاصة بكلمات المرور وتقارير المراقبة الخاصة باستخدام هذه الكلمات.

وتأتي مراعاة البنك لهذه الاعتبارات في إطار السياسة العامة التي تحكم تعاملاته مع العميل، والتي يأتي في مقدمتها بطبيعة الحال الحفاظ على سرية كافة البيانات الخاصة بالعميل، والتي من أهمها كلمة المرور الخاصة به[1].

ويجب أن تؤخذ التزامات البنك بخصوص التحكم في كلمة المرور سالفة الذكر في الاعتبار عند تقرير مسؤولية البنك عن انتهاك سرية كلمة المرور، بحيث يتحمل البنك المسؤولية عن كافة ما يحدث بسبب تقصيره في مراعاة هذه الأمور.

ويتضح لنا مما سبق أن كلمة المرور تلعب دورا كبيرا في نظام تأمين موقع البنك الإلكتروني، والعمليات المصرفية التي تتم من خلاله، فهي بمثابة صمام

---

(١) انظر أحد نماذج البنوك العاملة عبر شبكة الانترنت في الولايات المتحدة الأمريكية، والتي وضعت سياسة عامة تحكم الحفاظ على سرية البيانات المصرفية، انظر:

Bank of internet USA, Privacy Policy January 2006, available at: http://www. bankofinternet.com/privacy-policy.aspx

أمان ضد الدخول غير المشروع، على موقع البنك الإلكتروني، أو على الحساب الخاص بالعميل، والذي يعد من أكثر الانتهاكات خطورة وتهديدا لأمن البنك[1]، لذلك يجب أن تكون محل اهتمام من قبل البنك الإلكتروني، وذلك من خلال توفير إرشادات للعملاء ليستعينوا بها في اختيار كلمة المرور على نحو يجعلها صعبة التخمين من قبل الغير، أيضا توجيه العملاء إلى ضرورة المحافظة على هذه الكلمة من الاطلاع عليها. يجب على البنك الإلكتروني كذلك أن يمتلك حدًا أدنى من الرقابة والتحكم في نظام عمل كلمة المرور، على نحو يجعلها مؤمنة دائما.

ثانيا/ التشفير كوسيلة لتأمين رسائل البيانات بين البنك وعملائه:

٣١٥- يحتل التشفير[2] مكانة كبرى بين إجراءات تأمين معاملات البنك

---

(1) Graham Smith; Op. Cit, p. 278.

(٢) ويعرف علم التشفير بأنه العلم الذى يعنى بصياغة وانشاء زمرة متباينة من الشفرات التي تنضوى تحت دائرة كتابة الأسرار Secret Writing. وقد أمتد هذا العلم إلى تكنولوجيا المعلومات فأضحى يمثل فأصبح يمثل صمام أمان للبيانات لضمان عدم الدخول غير المرخص، أو إنشاء محتويتها أثنا ء عملية الانتقال بين الوسائط المعلوماتية المختلفة، بحيث يمتنع على غير المعنيين الاطلاع عليها. انظر ا. **حسن مظفر الرزو**؛ المرجع السابق، ص٧٣

- وتجدر الإشارة إلى استخدام الإنسان للتشفير منذ حوالي ألفي عام قبل الميلاد للحفاظ على سرية رسائله. وقد بلغ هذا الأستخدام ذروته في فترات الحروب؛ خوفا من وقوع الرسائل الخطيرة في يد الأعداء. وبعد أن ظهر الحاسوب تم استخدامه في إجراء التشفير وفك رموزه، وتجدر الإشارة إلى أن الحكومات في فترة الستينات احتكرت حق التشفير وفك التشفير. وفي أواخر الستينيات، أسست شركة (IBM) مجموعة تختص بأبحاث التشفير، ونجحت هذه المجموعة في تطوير نظام تشفير أطلقت عليه اسم لوسيفر (Lucifer)، وكان هذا النظام مثارا للجدل، حيث كان هناك العديد من التحفظات التي أثيرت حول إمكانية استخدام نظم التشفير من قبل الشركات والمؤسسات الخاصة. انظر: **د. سمير حامد الجمال**، مرجع السابق، هامش ص٢١٨.

الإلكتروني عبر شبكة الإنترنت(١)، وتأتى هذه المكانة من ملاءمة التشفير كوسيلة تأمين للمعاملات المصرفية الإلكترونية، بفضل ما تحققه من المحافظة على سرية وخصوصية المراسلات المتبادلة بين البنك وعملائه. يضاف إلى ذلك الاستخدامات المختلفة للتشفير في نظام عمل البنك، والتي تهدف جميعها إلى توفير الثقة في المعاملات المصرفية الإلكترونية.

ويقوم نظام العمل بالتشفير على استخدام أدوات أو وسائل لتحويل البيانات من شكلها الذي كانت عليه إلى شكل آخر (رموز رياضية غير مفهومة مثلا)، وذلك لإخفاء محتويتها، والحيلولة دون تعديلها أو استخدامها استخداما غير مشروع من قبل شخص غير مخول له باستعمالها(٢). وبالإضافة لذلك، يمكن من خلال التشفير التأكد من أن البيانات التي تسلمها المرسل إليه هي البيانات التي قام

---

(1) **Kit Burden**; Op. Cit, p. 249;

د. **حسين الماحي**، نظرات قانونية في التجارة الالكترونية: مرجع سابق، ص٢٩٨.

Jyske bank, JBPB, Net Bank user agreement, (EN)-2007, available at:

http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf

- ويعد تقديم خدمات التشفير واحدا من أهم الأهداف المعنية في السنوات الأخيرة لدى الحكومات المختلفة، وهذا ما أوضحه تقرير لجنة (Jack) في نهاية ١٩٨٨، والتي ذهبت إلى أن التشفير يشهد تطورا كبيرا، وأن من المتوقع أن تكون البنوك من أكثر المؤسسات التي يمكن أن تستفيد من ذلك من خلال تأمين المعاملات المصرفية الإلكترونية، بالنظر إلى التشفير على انه من انجع الوسائل للحفاظ على سرية وسلامة هذه المعاملات.

Graham Smith; Op. Cit, p. 278

د. **إسماعيل شاهين**، مرجع سابق، ص ٨.

(2) **Information Security**: Guide to the electronic communications Act. Available at:

www.berr.gov.uk/files/file9980.pdf

المرسل بإرسالها فعلاً، وذلك من خلال مجموعة من الوسائل الفنية التي تمكن المرسل إليه فقط من الاطلاع على محتوى الرسالة المرسلة(١).

وفى ظل هذه الأهمية التى يتمتع بها التشفير فى تأمين معاملات البنك، يقتضى الأمر التعرض لتعريفه وأنواعه، وكيفية إستخدامه، وذلك على التفصيل التالى:

١)- تعريف التشفير في نظام عمل البنك الإلكترونى:

٣١٦- عرف مشروع قانون التجارة الإلكترونية المصري في المادة الأولى(٢) التشفير بأنه عبارة عن "تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغيرها".

وعرف التشفير أيضا في القانون الفرنسي رقم ١١٧٠ الصادر بشأن تنظيم الاتصالات عن بعد في عام ١٩٩٠ بأنه عبارة عن "مجموعة الأعمال التي تهدف إلى تحويل بيانات أو إشارات واضحة عبر اتفاقات سرية، إلى بيانات أو إشارات غامضة للغير، أو إجراء العملية العكسية، وذلك عبر وسائل مادية أو معلوماتية مخصصة لهذا الغرض".

وقد وضع قانون الاتصالات الإلكترونية البريطاني الصادر في عام ٢٠٠٠ تعريفا ليس للتشفير ولكن "لخدمة دعم الشفرة"، حيث نصت المادة السادسة من

---

(١) د. **عبد الفتاح بيومى حجازى**، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الطبعة الأولى، ٢٠٠٥، ص ٣١؛ د. **عيسى غسان عبد الله الربضى**، القواعد الخاصة بالتوقيع الالكتروني، رسالة دكتوراه، كلية الحقوق – جامعة عين شمس، ٢٠٠٦، ص ٧٧

(٢) راجع مشروع القانون على الموقع الإلكتروني التالي:
http://www.f-law.net/law/showthread.php?t=13243

القسم الأول منه على ما يلى:

(١) في مفهوم هذا القسم فأن اصطلاح "خدمات دعم الشفرة" تعنى أي خدمة تقدم لمرسلى ومستقبلي الاتصالات الإلكترونية أو لهؤلاء الذين يخزنون البيانات الإلكترونية والمصممة لتسهيل استخدام تقنيات الشفرة للأغراض الآتية:

أ- ضمان أن تكون هذه الاتصالات أو البيانات من الممكن الدخول إليها أو أن توضع في شكل مفهوم للتعرف عليها من قبل أشخاص بعينهم.

ب- ضمان إمكانية التأكد من صحة وسلامة هذه الاتصالات أو البيانات[(١)].

وتعرض أيضا قانون المبادلات الإلكترونية التونسى رقم ٨٣ لسنة ٢٠٠٠ في الفصل الثاني من الباب الأول لتعريف التشفير، حيث عرفه بأنه "إما استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها".

ومفهوم التشفير في مجال عمل البنوك الإلكترونية العاملة عبر شبكة الإنترنت لا يختلف عن المفاهيم السابقة. فالتشفير أحد الوسائل الهامة لتأمين عمل البنك الإلكتروني عبر شبكة الإنترنت، وذلك من خلال استعمال هذه الوسيلة في تأمين المراسلات المتبادلة فيما بين البنك وعملائه، وذلك عن طريق استعمال رموز وإشارات تعمل إما على تغيير شكل البيانات المراد إرسالها على نحو يجعل من الصعب فهمها، أو استعمال رموز أو إشارات معينة بحيث لا يمكن

---

(١) مشار إلى هذه القوانين لدى **محمد أحمد محمد نور جستنية**، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق- جامعة القاهرة، ٢٠٠٥، ص ٢٢٧.

الوصول إلى هذه البيانات بدونها.

٢)- أنواع نظم التشفير في نظام عمل البنك الإلكتروني:

٣١٧- تبدو أهمية التعرض لأنواع نظم التشفير في التعرف على الطريقة الفنية التي يعمل بها كل نظام في علاقة البنك بعميله، حيث يتم تحديد النظام المتبع في ضوء تصميم الشبكة الداخلية للبنك، يضاف إلى ذلك، أنه يقع على البنك التزاما قانونيًا ـ تقتضيه طبيعة الاتصال الإلكتروني عن بعد (١٤٨ مدني مصري) ـ بإعلام العميل بالتفاصيل الفنية لنظام التشفير المتبع في المراسلات الإلكترونية التي تتم فيهما بخصوص المعاملات المصرفية، والتي غالبا ما يقوم البنك بتوضيحها للعميل، إما من خلال عرضها على الموقع الإلكتروني له، أو بالنص عليها في العقد المصرفي الذي ينظم العلاقة بينهم(١).

---

(1)**Sofia Giannakoudi**; **Op. Cit, p.** 210; **Everett Durante Cordy**; Op. Cit, p. 405

د. **حسين الماحي**، نظرات قانونية في التجارة الإلكترونية، مرجع سابق، ص٢٩٨.

Jyske bank, JBPB, Net Bank user agreement, (EN)-2007, available at:

http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf

- ويعد تقديم خدمات التشفير واحدا من أهم الأهداف المعنية في السنوات الأخيرة لدى الحكومات المختلفة، وهذا ما أكد عليه تقرير لجنة (Jack) في نهاية ١٩٨٨؛ والتي ذهبت إلى أن التشفير يشهد تطورا كبيرا، وأن من المتوقع أن تكون البنوك من أكثر المؤسسات التي يمكن أن تستفيد من ذلك من خلال تأمين المعاملات المصرفية الإلكترونية، بالنظر إلى التشفير على أنه من أنجع الوسائل للحفاظ على سرية وسلامة هذه المعاملات.

Graham Smith; Op. Cit, p. 278

د. **إسماعيل شاهين**، مرجع سابق، ص ٨.

هذا ويوجد نوعان من نظم التشفير المستخدمة على التفصيل التالى:

١- التشفير بالمفتاح المتماثل (Symmetric Key Encryption):

وفي هذا النظام من نظم التشفير يستخدم كل من المرسل والمستقبل مفتاحًا سريًا واحدًا لتشفير الرسالة وفك تشفيرها، وذلك من خلال الخطوات التالية[١]:

أ – بداية يتفق كل من البنك الإلكتروني والعميل على كلمة مرور(عادة ما يتم اختيار كلمة طويلة، أي تحتوى على حروف ورموز كثيرة)، حيث يتم إدخال هذه الكلمة على النص المراد تشفيره من خلال برمجيات التشفير.

ب- تعمل برمجيات التشفير بعد ذلك على تحويل هذه الحروف والرموز إلى عدد ثنائى، ثم يتم إضافة رموز أخرى لزيادة طولها، حيث يشكل العدد الثنائى الناتج مفتاح تشفير الرسالة.

ج- بعد ذلك يتم إرسال الرسالة من المرسل إلى المستقبل (سواء من العميل إلى البنك أو العكس). وبعد وصول الرسالة يستخدم المستقبل عبارة المرور نفسها من أجل فك شفرة النص المشفر، حيث تعمل البرمجيات على تحويل النص المشفر إلى شكله الأصلى المفهوم.

ويعتمد التشفير المتماثل على العديد من المعايير التي يتم التشفير من خلالها ومن أشهر هذه المعايير معيار يسمى (DES)[٢].

(١) انظر هذه المقالة على العنوان التالي:
http://www.itep.ae/arabic/EducationalCenter/Articles/Encryption_03.asp#3

(٢) ويستخدم هذا المعيار من معايير التشفير على نطاق واسع، وقد تم اعتماد هذا المعيار

وقد ظهرت العديد من مثالب استخدام نظام التشفير بالمفتاح المتماثل على نحو دفع إلى اللجوء الى وسائل آخري، ومن هذه المثالب:

- أنه يجب أن يكون مفتاح التشفير موجودا لدى كل من الطرفين اللذين يتبادلان البيانات، مما يدفعهم إلى تبادل المفتاح السرى بينهما على نحو قد يؤدى إلى سرقته أثناء عملية التبادل (وذلك على فرض أن كلا من الجهازين يقع تحت التجسس)(١).

- يضاف إلى ذلك أن المتنصت يستطيع فك شفرة أي رسالة يتم تبادلها بين المتعاملين، وذلك بعد التوصل إلى المفتاح السرى لأحد المتعاملين من خلال الشيء جهازه، حتى ولو لم يقم بذلك مع الطرف الأخر؛ حيث إن المفتاح المستخدم للتشفير وفك التشفير واحد.

٢- التشفير بالمفتاح غير المتماثل:

يقف وراء اللجوء إلى التشفير بالمفتاح غير المتماثل مشكلة التوزيع غير الآمن للمفاتيح في التشفير المتماثل، حيث تقوم فكرة التشفير غير المتماثل على الاستعاضة عن المفتاح الواحد للتشفير بمفتاحين مرتبطين، يسمى أحدهما بالمفتاح

للتشفير من قبل الحكومة الأمريكية منذ عام ١٩٧٦. لكن هذا المعيار أظهر ضعفا خلال السنوات الأخيرة أمام أساليب كسر التشفير، وبدأت تستبدل في عدة أماكن بنسخ معدلة عنها مثل معيار يسمى Triple DES، إلا أن DES استبدلت كليا كمعيار معتمد في الحكومة الأمريكية في نهاية عام ٢٠٠١ بمعيار أفضل AES (Advanced Encryption Standard. انظر **أحمد الهاشمي**، التشفير بالمفتاح المتناظر، مقالة على شبكة الانترنت متاحة على العنوان التالى:
http://www.boosla.com/showArticle.php?Sec=Security&id=35

(١) المرجع السابق.

العام ((public key) [1] والآخر بالمفتاح الخاص (private key)[2]، بحيث يكون المفتاح الخاص معروفا لدى جهة واحدة أو شخص واحد وهو المرسل، حيث يستطيع بموجب هذا المفتاح الخاص أن يقوم بتشفير الرسالة وفك شفرتها. أما المفتاح العام فيكون معروفا لدى أكثر من شخص أو جهة، وبموجب هذا المفتاح العام يمكن فك شفرة الرسالة التي شفرها المفتاح الخاص، كما يمكن استخدامه أيضا لتشفير رسالة مرسلة لمالك المفتاح الخاص. لكن لا يمكن استخدام المفتاح العام لفك شفرة رسالة شفرها هذا المفتاح العام، إذ إن مالك المفتاح الخاص فقط هو الذي يستطيع فك شفرة الرسالة المشفرة بالمفتاح العام.

ويعد التشفير بأسلوب المفتاح غير المتماثل أكثر أمانا من التشفير بأسلوب التشفير بالمفتاح المتماثل، إلا أن الأسلوب الأول أكثر بطئا من الثاني[3].

---

(١) وتشير كلمة المفتاح (Key) إلى قيمة رياضية عبارة عن مجموعة كبيرة من الأرقام تستخدم كخوارزميات تشفير (cryptographic algorithms)، بحيث يمكن من خلالها تشفير الرسالة الإلكترونية وحل شفرتها. انظر:

Michael Chissick, Alistair Kelman, Op, Cit, p. xiII.

(٢) ويعد نظام (**RSA**) من أشهر نظم التشفير المتماثل، وقد اخترع هذا النظام عام ١٩٧٧ من قبلR. rivest, A.shamir وهو يستخدم في مجالات التوثيق المختلفة.

Michael Chissick, Alistair Kelman, Op, Cit, p. xlii.

(3) **Background report on electronic commerce 1998**; Op. Cit, p. 119.

- انظر أيضا الموقع الإلكتروني التالي:

http://www.itep.ae/arabic/EducationalCenter/Articles/Encryption_04.asp#4

٣)- كيفية استخدام التشفير في علاقة البنك الإلكتروني والعميل:

٣١٨- وتتم عملية التشفير بصورة عملية في علاقة البنك الإلكتروني والعميل من خلال مرحلتين: الأولى: الاتفاق بين البنك الإلكتروني والعميل على أدوات التشفير، والثانية: مرحلة نقل البيانات، وذلك على النحو التالي:

الأولى- الاتفاق بين البنك الإلكتروني والعميل على أدوات التشفير:

يتم في هذه المرحلة الاتفاق بين البنك الإلكتروني والعميل على أدوات التشفير التي سيتم استخدامها في عملية التشفير. وهذا الاتفاق يتضمن تحديد مجموعة الخوارزميات[١] (Algorithms) التي ستستخدم لحماية البيانات المتبادلة، والموافقة كذلك على مجموعة مفاتيح التشفير (cryptographic keys)، وأيضا الوسيلة التي تمكن البنك من التحقق من شخصية العميل والعكس.

الثانية- مرحلة نقل البيانات:

بمجرد الانتهاء من مرحلة الاتفاق بين البنك الإلكتروني والعميل سالفة الذكر، يتم استخدام الأدوات السالفة الذكر في نقل البيانات بينهما. حيث تعمل هذه الأدوات على تقسيم الرسالة المراد إرسالها إلى أجزاء، وتنقل في صورة سلسلة من السجلات المؤمنة، حيث يحمل كل سجل منها رقمًا سريًا معينًا، وعندما تصل

---

(١) والخوارزميات عبارة عن معادلات رياضية معقدة جدا تعمل على تشفير الرسالة من خلال تحويلها من شكلها الأصلي إلى ملخص، على أن يتم تحويل هذا الملخص إلى الشكل الأصلي مرة أخرى عند حل شفرة الرسالة. انظر **محمد سعيد أحمد إسماعيل**، المرجع السابق. ص١٩٠.

الرسالة يتم تجميع هذه الأجزاء من خلال أدوات لفك الشفرة[1].

وهكذا يتضح لنا مدى أهمية التشفير في عمل البنك الإلكتروني بصورة عامة، سواء لتأمين البيانات المتبادلة بين البنك الإلكتروني والعميل، أو لتأمين البيانات المتبادلة بين الأجهزة العاملة في شبكة البنك الإلكتروني.

---

(1) **M. Sklira. A.S.pomportsis. M.S. Obaidat,** Op, Cit, p. 1778.

- يمكن أن يظهر التشفير من خلال تطبيقات متعددة في نظام عمل البنك الإلكتروني، وذلك على النحو التالي:

١- تشفير الوصلات Transmission Level الخاصة بشبكة البنك الإلكتروني:

من خلال هذا المستوى يتم تشفير كل ما يمر من بيانات عبر وصلات الاتصالات الخاصة بشبكة البنك الإلكتروني، والتي تربط أجهزة الشبكة ببعضها، بحيث تبدأ عملية التشفير عند نقطة الإرسال، على أن يتم حلها عند نقطة الاستقبال.

٢- تشفير عملية التصفح Session Level التي تتم عبر موقع البنك الإلكتروني:

يتم التشفير من خلال هذا المستوى للبيانات التي يتم تداولها بين برنامج تصفح البيانات الموجود على الصفحة الرئيسة لموقع البنك الإلكتروني، والتطبيقات المختلفة الخاصة بالعمليات المصرفية.

٣- تشفير تطبيقات (Application Layer) العمليات المصرفية الإلكترونية:

وهذا المستوى من مستويات التشفير يتم من خلال تشفير جزئي لكل تطبيق من التطبيقات الخاصة بالعمليات المصرفية الإلكترونية الموجودة على موقع البنك الإلكتروني. والمثال على هذه النظم. نظام تشفير الصفقات الإلكترونية الآمنة (Secure Electronic Transaction) ونظام محفظة سيبر كاش (Cyber Cash Wallet).

٤- تشفير الملفات الموجودة على أجهزة البنك الإلكتروني:

من خلال هذا المستوى من مستويات التشفير يتم تشفير الملفات الموجودة داخل أجهزة البنك الإلكتروني خاصة الملفات التي تتضمن بيانات سرية، بحيث لا يتمكن من الدخول على هذا الملفات إلا الأشخاص القائمون على تشغيل البنك، وبضوابط معينة نظرا لخطورة هذه البيانات. انظر هذه التطبيقات. **رأفت رضوان**، المرجع السابق، ص ٨٢.

وانطلاقا من هذه الأهمية يجب على البنك أن يتبنى أفضل طرق التشفير الموجودة في العمل، وأن يحرص دائما على التزود بأفضل ما تم التوصل إليه في هذا المجال، وأن يزود العميل دائما بنظم التشفير الحديثة، وأن يحرص على أن يمده بما يمكنه من استعمال هذه النظم على وجه سليم.

ثالثا/ الخوائط النارية كوسيلة لتأمين الموقع الإلكتروني للبنك:

٣١٩- دخلت الحوائط الناريةFirewalls إلى الاستخدام في مجال تأمين المواقع الإلكترونية على شبكة الإنترنت بصورة كبيرة في الآونة الأخيرة(١)، وهو تعبير يشابه ما كانت تقوم به القبائل في العصور القديمة من عمل دوائر نيرأن حول أماكن تمركزها لتمنع الأعداء من الوصول إليها(٢).

وتلعب الحوائط النارية دورا محوريا في مجال تأمين شبكة البنك الإلكتروني(٣)؛ حيث تعمل كحاجز أو حائط صد في مواجهة جميع المسارات القادمة للبنك من على شبكة الإنترنت، وذلك من خلال التأكد والتحقق من مصدر هذه المسارات، ثم تحديد ما إذا كان يسمح لها بالمرور من عدمه(٤).

وتعرف هذه الحوائط بأنها عبارة عن مجموعة الأجهزة والبرامج التي تعمل

---

(1) **G C Chalikias**, Op, Cit, p. 58.

(٢) **د. إسماعيل شاهين**، مرجع سابق، ص ٨؛ **رأفت رضوان**، عالم التجارة الإلكترونية، المرجع السابق، ص١٠٩؛

E-Banking, Federal Financial Institutions Examination Council; Op. Cit, p. 5

(3) **G C Chalikias**, Op, Cit, p. 58; **Oliver Lau**, Meta-Firewall: A Sixth Generation Firewall, Elsevier Science Ltd, 1998, p. 14.

(4) **M. Sklira. A.S.pomportsis. M.S. Obaidat**, Op, Cit, p. 1778.

كحاجز أو مانع بين شبكة البنك الإلكتروني وشبكة الإنترنت، وذلك لحماية البنك (شبكة البنك، الأجهزة، البرامج، خطوط الاتصال) ضد كافة أشكال الانتهاكات التي تستهدف أمنه وذلك من خلال تنظيم الاتصالات وتبادل البيانات بين البنك الإلكتروني وشبكة الإنترنت، والعمل على مراقبة عمليات الدخول على نحو يمكن معه اكتشاف أي عملية استخدام غير مخول (Unauthorized usage) أو تعامل مشكوك فيه (Suspicious dialogues)[١].

وتعمل الحوائط النارية على ترشيح (Filter) وتصفية كافة الطلبات القادمة للبنك الإلكتروني عبر شبكة الإنترنت، وذلك قبل أن يسمح لها بالوصول إلى خادم التطبيقات لدى البنك، حيث تعمل على ترتيب هذه الطلبات، وتنظيم دخولها، بحيث لا يسمح بالوصول إلا للطلبات الموثوق بها والتي يعرف مصدرها مثل صفحات الويب العائدة (Retrieving web pages) إلى البنك بعد ملء ما بها من بيانات من قبل العملاء الطالبين لخدمة مصرفية معينة، أو طلبات العملاء المرسلة للبنك الإلكترونى[٢]، ثم تعمل الحوائط النارية بعد ذلك على تغيير عنوان الطلبات أو المسارات ثم تقوم بتسليمها للموقع المناسب، وبهذه الطريقة يتم حماية العناوين الداخلية من الدخول المباشر عليها، وكذلك حماية شبكة البنك بحيث تكون مختفية عن المراقبين الخارجيين (Invisible to outside

(١) د. إسماعيل شاهين، مرجع سابق، ص ٨؛

Zakaria I.Saleh; Op, Cit, p. 18; **G C Chalikias,** Op, Cit, p. 59;

- available at: http://www.echeck.org/library/glossary.html.

(2) **America California Bank's Principles of Privacy**, article, available at :

http://www.acbank.com/privacy.html

.[1](observers

---

(1) **M. Sklira. A.S.pomportsis. M.S. Obaidat**;Op, Cit, p. 1778.

- ويوجد نوعان من الحوائط النارية وهما:

أ- **مرشحات مجموعة البيانات Packet Filters**:

وتقوم مرشحات مجموعة البيانات باختبار كل حزمة بيانات قادمة أو خارجة كي يتم التعرف على مدى مطابقتها للقواعد الحاكمة لنظام العمل على شبكة البنك الإلكترونى وذلك كما لو كانت القواعد التي تحكم الدخول على موقع البنك الإلكتروني تمنع دخول أي حزم بيانات محملة ببرامج تعمل على تدمير الموقع أو سرقة ما به من بيانات، ومن ثم تقوم مرشحات مجموعة البيانات في هذه الحالة بمنع مثل هذه الحزم من الدخول.

ب- **تطبيقات التحكم في البوابات Application Gateways**:

و تعمل هذه التطبيقات على حاسبات خاصة لنظم أمن المواقع. وهذه التطبيقات بالإضافة إلى قيامها بعمل المرشحات لمجموعات البيانات، تقوم أيضا بالحجب الكلى للعناوين الداخلية للبنك الإلكترونى، بحيث لا ترى الجهات الخارجية إلا الصفحة الرئيسة لموقع البنك الإلكترونى، على نحو تظهر معه كافة تعاملات البنك الإلكتروني بعنوان الصفحة الرئيسة لموقع البنك الإلكتروني فقط، ومن ثم تمنع أي محاولة خارجية للنفاذ إلى المكونات الداخلية لموقع البنك الإلكترونى، كما تعمل على التحكم في الأدوات الأمنية لكافة التطبيقات الخاصة بالعمليات المصرفية كي تسمح فقط للأطراف الشرعيين أو المخول لهم (authorized parties) بالدخول إلى هذه التطبيقات.

رأفت رضوان، عالم التجارة الإلكترونية، المرجع السابق، ص١٠٩؛ انظر أيضا:

G C Chalikias; Op. Cit, p. 59; **Thomas C. Glaessner, Tom Kellermann, Valerie McNevin**; Op, Cit, p. 69.

المطلب الثانى

التزامات جهة التوثيق في مواجهة البنك الإلكتروني

٣٢٠- يجرى عمل البنوك العاملة عبر شبكة الإنترنت على إلزام جهة التوثيق بتقديم بعض خدماتها (كإصدار شهادة توثيق) لصالح عميل البنك، وذلك بموجب اتفاق خاص يدرج بالعقد الذي يحكم علاقة البنك بجهة التوثيق. ويلجأ البنك إلى هذا الأمر؛ حتى يضمن أن توثيق العميل قبل تعامله معه قد تم بمعرفة جهة توثيق يتعامل معها ويثق فيها[١].

ويمكن القول بصدد تكييف إلزام البنك لجهة التوثيق بتقديم مثل هذه الخدمات لصالح عميله بأنه اشتراط لمصلحة الغير[٢]، حيث يتعاقد البنك باسمه (لا باسم العميل) مع جهة التوثيق لإعطاء العميل حقا مباشرا في مواجهة جهة التوثيق مصدره العقد (بين البنك وجهة التوثيق)، تحقيقا لمصلحة مشروعة للبنك تتمثل في ضمان توثيق العميل عن طريق جهة يثق فيها.

---

(١) وتعتبر خدمة التوثيق على هذا النحو خدمة يقدمها البنك الإلكتروني لعميله (وإن كان بطريق غير مباشر) ويمكن للبنك أن يحصل على مقابل هذه الخدمة من العميل، أو أن تتقاضى جهة التوثيق المقابل المالي من العميل مباشرة. انظر:

Authentication in an electronic banking environment; Op. Cit, p. 8.; **William Gram**; Op. Cit, p. 8.

(٢) ينص **القانون** المدني المصري في المادة ١٥٤ على أن "يجوز للشخص أن يتعاقد باسمه على التزامات يشترطها لمصلحة الغير إذا كان له في تنفيذ هذه الالتزامات مصلحة شخصية مادية كانت أو أدبية".

وبموجب التعاقد الذي يتم بين البنك وجهة التوثيق تلتزم الأخيرة بمجموعة من الالتزامات على النحو التالي:

١) تزويد البنك الإلكتروني بالأجهزة والبرامج اللازمة لتأمينه:

٣٢١- يأتي في مقدمة التزامات جهة التوثيق تجاه البنك الإلكتروني أن تسلمه كافة الأجهزة والبرامج اللازمة لتأمين موقعه على شبكة الإنترنت، وكذلك التعاملات التي تتم عبر هذا الموقع. ويتحقق هذا الالتزام من خلال قيام جهة التوثيق بتمكين البنك الإلكتروني من حيازة هذه الأشياء على نحو يتمكن معه البنك من الاستفادة منها، والقيام بربط هذه الأجهزة والبرامج بالشبكة الداخلية للبنك وموقعه على شبكة الإنترنت، وقيام جهة التوثيق بتسليم البنك الإلكتروني، مثل هذه الأدوات قد يكون على سبيل التمليك أو فقط على سبيل الانتفاع وذلك وفقا لما يتم الاتفاق عليه بين الطرفين(١).

هذا وقد خلا قانون التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤ من النص على هذا الالتزام صراحة، لكن كراسة شروط ومتطلبات منح تراخيص تقديم خدمات التوقيع الإلكتروني الصادرة عن هيئة تنمية صناعة تكنولوجيا المعلومات، تعرضت له في المادة ١٠ فقرة (١) بصورة غير مباشرة، وذلك عندما عالجت اختصاصات جهة التوثيق، حيث ذكرت أنه "يجب على الجهة المرخص لها (جهة التوثيق) أن تزود المستخدمين النهائيين (البنك الإلكتروني) بأدوات إنشاء التوقيع الإلكتروني (البطاقة الذكية + القارئ)(٢).

---

(١) د. محمد حسين منصور، مرجع السابق، ص٩٧.

(٢) كراسة شروط ومتطلبات منح تراخيص تقديم خدمات التوقيع الإلكتروني الصادرة عن هيئة تنمية صناعة تكنولوجيا المعلومات، مرجع سابق، ص ١٠.

والملاحظ على النص السابق أنه قصر الأدوات التي تلتزم جهة التوثيق بتقديمها للبنك على أدوات التوقيع الإلكتروني فقط. وهذا يتفق مع النظرة الضيقة التي تبناها المشرع المصري لخدمات التوثيق الإلكتروني.

وعلى صعيد التشريعات الأخرى، نلاحظ أن قانون التوثيق الإلكتروني الأمريكي حرص على تنظيم هذا الالتزام، وذلك من خلال النص على التزام جهة التوثيق بتزويد البنك بكافة الأدوات والبرامج اللازمة لتأمين وجود البنك وتشغيله على شبكة الإنترنت[1].

هذا وقد تواترت التشريعات الأمريكية الخاصة بحماية سرية البيانات ("HIPAA Act"[2] "GLB Act"[3] ."COPPA"[4]) على استعمال عبارة خاصة لبيان طبيعة الأدوات التي يجب على جهة التوثيق أن تزود البنك بها، وهي أن تكون "أدوات تجارية مناسبة commercially reasonable means"[5].

---

(1) **Digital signature and electronic authentication law (SEAL) of 1998 (Introduced in Senate),** available at: http://thomas.loc.gov/cgi-bin/query/z?c105:S.1594.IS

(٢) هذا القانون متاح على الموقع الإلكتروني التالي:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

(٣) هذا القانون متاح على الموقع الإلكتروني التالي:

http://frwebgate.access.gpo.gov/cgi-

(٤) هذا القانون متاح على الموقع الإلكتروني التالي:

www.ftc.gov/ogc/cOppa1.pdf

(5) **David L. Baumer and others**; Op. Cit, p. 409.

ولعل هذه العبارة تعكس دلالات خاصة يجب أن تؤخذ في الاعتبار من قبل جهة التوثيق عند تزويد البنك بالأدوات الفنية اللازمة لتأمينه هذه الدلالات تظهر في استشعار هذه القوانين لأهمية وخطورة المعاملات التجارية بصورة عامة والمصرفية بصورة خاصة بالمقارنة بغيرها من المعاملات الأخرى التي تتم على شبكة الإنترنت، ومن ثم يجب أن تأتي الأدوات الأمنية ملائمة للطبيعة الخاصة لهذه المعاملات، وذلك من حيث ارتفاع مستوى التأمين، وانتقاء أفضل أنواع الأجهزة لذلك.

ويتفرع عن التزام جهة التوثيق بتسليم هذه الأجهزة والبرامج للبنك التزام بتسليم ملحقات هذه الأشياء، والتي من أهمها كافة المستندات والوثائق الشارحة لنظام عمل الأجهزة والبرامج، وأساليب الصيانة. وتتمثل هذه المستندات والوثائق في كتيبات، أو اسطوانات، أو معلومات تنقل عبر الشبكة، أو دورات تدريبية(١).

وهذا الالتزام يجد له أصلاً في القواعد العامة في القانون المدني المصري، تلك التي تقضي في المادة ٤٣٢ بأن " يشتمل التسليم ملحقات الشيء المبيع وكل ما أعد بصفة دائمة لاستعمال هذا الشيء وذلك طبقا لما تقضي به طبيعة هذا الشيء وعرف الجهة وقصد المتعاقدين"

ولعل الصيغة العامة التي هيمنت على عبارات النص السابق كفيلة باستيعاب التزام جهة التوثيق بتسليم ملحقات أجهزة التأمين للبنك، وذلك في ضوء طبيعة هذه الأجهزة والغرض المبتغى منها.

---

(١) **عزة محمود أحمد**، مرجع سابق، ص١٢٧؛ د. **سعيد سعد عبد السلام**، مرجع سابق، ص١١٢؛ د. **نبيلة إسماعيل** رسلان، مرجع سابق، ص١٦،١٥.

أيضا أبرز التوجيه الأوربي [1] هذا الالتزام والذي يرتبط ارتباطا لا يقبل التجزئة بالتزام جهة التوثيق بتسليم الأجهزة والبرامج اللازمة لتأمين البنك.

وتلتزم جهة التوثيق بتسليم هذه الأجهزة والبرامج مطابقة للمواصفات الفنية والمتفق عليها في العقد والتي تتناسب مع تأمين وجود وعمل البنك على شبكة الإنترنت. وهذا ما عالجته القواعد العامة في القانون المدني المصري، حيث جاء في عجز المادة ٤٣١ نص "بالتزام البائع بتسليم المبيع وملحقاته بالحالة التي كان عليها وقت البيع..." . لكن يجب الإشارة إلى أمر هام وهو أن التسليم هنا ليس عملا ماديا يتم من خلال وضع الأجهزة والبرامج تحت سيطرة البنك وحسب، بل يجب أن توفر جهة التوثيق للبنك الفنيين المتخصصين لتركيب وتشغيل هذه الأجهزة والبرامج، ومراعاة تناسب هذه الأجهزة من حيث الكم والكيف مع حجم تعاملات وأنشطة البنك والتأكد من صلاحيتها للعمل. والحكم على مدى مطابقة هذه الأجهزة والبرامج للمواصفات يقتضي وضعها تحت التجربة لفترة معينة للتأكد من صلاحيتها وسلامتها، وذلك قبل أن يقوم البنك بالتوقيع على المستند الخاص بالاستلام [2].

والتزام جهة التوثيق بتسليم الأجهزة والبرامج للبنك الإلكتروني في المكان

---

(1) **Directive** 2002/58/EC, (Directive on privacy and electronic communications), Official Journal of the European Communities, item (20):
(... It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks, which lie outside the scope of possible; remedies by the service provider.

(٢) د. **محمد حسين منصور**، مرجع السابق، ص ١٠١، ١٠٢

والزمان وطبقا للمواصفات المتفق عليها هو التزام بتحقيق نتيجة (ما لم ينص الاتفاق على غير ذلك) بمعنى أن جهة التوثيق لا تبرأ ذمتها في مواجهة البنك إلا بتحقيق استفادة البنك الفعلية من هذه الأدوات، بحيث تنعقد مسؤوليتها في حالة عدم قيامها بتسليم هذه الأشياء، أو تسليمها متأخرة، أو غير مطابقة للمواصفات المتفق عليها. ويمكن في حالة امتناع جهة التوثيق عن ذلك أن يتم اللجوء إلى التنفيذ العيني، وذلك في الحدود التي يكون فيها هذا التنفيذ ممكنا، مع الأخذ في الاعتبار الطبيعة الفنية لمحل الالتزام ومدى قابليته للتنفيذ العيني(١).

- كذلك تلتزم جهة التوثيق في مواجهة البنك الإلكتروني بأن تزود عميله بكافة الأجهزة والبرامج الخاصة بعمليات التشفير والتوقيع الإلكتروني وغيرها من الوسائل التي تلزم لتأمين تعاملاته مع البنك ويجب أن تضمن جهة التوثيق في مواجهة البنك الإلكتروني توافر أعلى درجات الأمان والسلامة في هذه الأجهزة.

وعادة ما ينص البنك الإلكتروني في تعاقداته مع العميل على أن تظل هذه الأجهزة والأدوات ملكا للبنك، وتحظر على العميل أن يتصرف في هذه الأجهزة(٢).

ويلتزم العميل في استعماله لهذه الأجهزة والبرامج بالحفاظ عليها واستعمالها وفقا للتعليمات والتوجيهات التي توصى بها جهة التوثيق، ويكون هو المسئول عن أي فقد أو تلف يحدث لهذه الأدوات والبرامج. ويلتزم العميل كذلك بالحفاظ

(١) **تنص المادة ١/٢٠٣ من القانون المدني المصري** على أن " يجبر المدين بعد إعذاره طبقا للمادتين ٢١٩، ٢٢٠ على تنفيذ التزامه عينيا متى كان ذلك ممكنا".

(2) (The equipment shall at all times remain the property of the bank and the customer shall not in any circumstances obtain any rights over, or in, the same) See: **MCB INTERNET BANKING**, available at: http://www.mcb.mu/documents/terms/ibterms. html

على كل ما يرتبط بعمل وتشغيل هذه الأجهزة والبرامج من بيانات تكون لازمة لعملها كأرقام سرية، أو أرقام تعريف، كما يلتزم بإبلاغ البنك فور تعرض مثل هذه البيانات للسرقة أو الاطلاع عليه من قبل شخص غير مسموح له بذلك(١).

والسؤال: ماذا لو حدث واضطر عميل البنك إلى الاستعانة ببعض الأجهزة أو البرامج التي قد لا تتوافر لدى جهة التوثيق لظروف قد تتعلق بطبيعة أو حجم نشاطه مثلاً؟

ذهبت بعض الاتفاقات الموضوعة من قبل أحد البنوك العاملة عبر شبكة الإنترنت (MCB INTERNET BANKING) إلى تنظيم هذا الفرض، حيث ذهبت إلى أن عمل هذه الأجهزة والبرامج يكون محكومًا بالعقد المبرم بين هذا العميل والجهة التي حصل منها على هذه الأجهزة والبرامج(٢). أي أن الجهة التي حصل منها العميل على الأجهزة والبرامج هي المسئولة عن تمكين العميل من الاستفادة من هذه الأجهزة بالكم والكيف الذي يتناسب مع طبيعة وحجم نشاط هذا

---

(1) (The Customer shall effect and maintain adequate measures to safeguard and not part with possession of any of the equipments, and notify the Bank immediately on becoming aware of any unauthorized use or possession thereof, or of any claims by a third party in relation to the Customer's use or possession thereof)
MCB INTERNET BANKING, available at:
http://www.mcb.mu/documents/terms/ibterms.html

(2) (The use of and/or downloading of any file/software from the Internet, be it from the MCB I.B. Site or not, shall be at his own risk and shall be subject to the terms and conditions imposed by the licensor of the software which in all cases, shall be considered as third party's software.)
Ibid.

العميل، لكن يجب عليها أن تراعى في ذات الوقت طبيعة الأنشطة المصرفية للبنك. ويبدو لنا أنه حتى في هذا الفرض يجب على البنك وأن يقبل ويوافق على هذا الأمر، وذلك حتى يتأكد من موثوقية الجهة التي حصل منها العميل على هذه الأجهزة.

٢) الحفاظ على سرية البيانات الخاصة بالبنك الإلكتروني والعميل(١):

٣٢٢- يصور نشاط البنك الإلكتروني العامل على شبكة الإنترنت على أنه عبارة عن نشاط مكثف للبيانات، يقوم على معالجة داخلية للبيانات الشخصية والمالية، ثم التوزيع الخارجي لهذه البيانات بين البنك الإلكتروني والعميل. وقد اقتضت طبيعة هذا النشاط ضرورة فرض الالتزام بحماية سرية هذه البيانات، ليس فقط من قبل أطراف المعاملات المصرفية (البنك الإلكتروني والعميل)، ولكن أيضا من قبل جهة التوثيق التي تستطيع الاطلاع على هذه البيانات بحكم طبيعة عملها(٢).

ويقصد بهذا الالتزام تعهد جهة التوثيق بالحفاظ على سرية المعاملات التي تتم بين البنك الإلكتروني والعميل بكل ما تتضمنه هذه المعاملات من بيانات

---

(١) كلمة السرية ليس لها تعريف محدد، لكن يمكن أن تعرف بأنها عبارة عن قدرة الفرد أو مجموعة من الأفراد على الحفاظ على جوانب معينة من حياتهم وشئونهم الشخصية بعيدا عن عموم الناس عنها، أو السيطرة على تدفق المعلومات الخاصة بهم. والسرية تنطوي على شيء مجهول بالنسبة للكافة؛ نظرا لكونها ذات قيمة كبيرة بالنسبة للأشخاص الذين يعرفونها. والسرية يمكن أن ينظر إليها على أنها جانب هام من جوانب الأمن الإلكتروني. انظر:

Privacy, From Wikipedia, the free encyelopedia, available at:

(2) **Apostolos Ath. Gkoutzinis**; Op. Cit, p. 179.

William Gram; Op. Cit, p. 9.

شخصية وأرقام الحسابات وغيرها من البيانات التي تطلع عليها جهة التوثيق بحكم ممارستها لعمليات تأمين البنك(١).

ويبدو للوهلة الأولى وجود شيء من التعارض بين التزام جهة التوثيق بالقيام بعملية التحقق من شخصية العميل والذي يفرض عليها ضرورة الاطلاع على بيانات العميل الشخصية من خلال تجميع هذه البيانات والاستدلال والتأكد من صحتها على نحو يتيح التعرف على هوية هذا العميل، وبين التزامها بالحفاظ على السرية؛ والذي يفرض عليها عدم الاطلاع على البيانات الخاصة بمعاملات البنك مع العملاء.

لذلك يجب على جهة التوثيق عند قيامها بمثل هذه العمليات ألا تطلع على هذه البيانات إلا بالقدر اللازم فقط لإتمام عملية التوثيق، وذلك من خلال الحد من عمليات الاطلاع إلى أقصى درجة ممكنة. يضاف إلى ذلك التزام جهة التوثيق عند اختيار العاملين لديها الذين لهم احتكاك مباشر بهذه البيانات بعناية شديدة؛ بأن يكونوا أهلا للثقة، وأن تشدد في التنبيه عليهم بضرورة توخي الحرص الشديدوالحذر عند التعامل مع هذه البيانات؛ وضرورة فرض نوع من الرقابة على هؤلاء العاملين أثناء عملهم(٢).

---

(١) **د. جمال عبد الرحمن محمد على**، الخطأ في مجال المعلوماتية، مرجع سابق، ص٨٨؛ انظر أيضا: **د. محمد حسام محمود لطفي**، عقود خدمات المعلومات، دار النهضة العربية، ١٩٩٤، ص ١٤٦.

(2) **Principles for Electronic Authentication**, The Authentication Principles Working Group, E-Commerce Branch Industry Canada, p. 9.
www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Authentication.pdf/$file/Authentication.pdf

وعن الوضع في مصر فقد نص المشرع المصري في القانون رقم ١٥ لسنة ٢٠٠٤ الخاص بالتوقيع الإلكتروني في المادة ٢١ منه على أن "بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات الترخيص الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله".

والملاحظ على الوضع في القانون المصري أنه قصر فرض الالتزام بالسرية على جهة التوثيق فقط في حالة التوقيع الإلكتروني، دون أنشطة التوثيق الإلكتروني الأخرى، وذلك كما فعلت القوانين الأخرى التي مدت هذا الالتزام ليشمل كل أنشطة التوثيق، وذلك بحكم أن هذا القانون صدر لينظم أحكام التوقيع الإلكتروني فقط.

فقد أبرز التوجيه الأوربي(١) في أكثر من موضع أهمية التزام جهة التوثيق

Davis, Jessica, Radosevich, Lynda, Safeguarding data, Vol. 21, Issue 8, Academic Search Complete, p. 62.

http://www.ebscohost.com/thisTOpic.php?marketID=1&tOpicID=633

(1) **Directive** 1999/93/EC Official Journal of the European Communities, December 1999, article (24): (In order to increase user confidence in electronic communication and electronic commerce, certification service- providers must observe data protection legislation and individual privacy).

Directive 2002/58/EC, (Directive on privacy and electronic communications), Official Journal of the European Communities, Article 1 (Scope and aim):

(This Directive harmonizes the provisions of the Member States

بالمحافظة على سرية البيانات الخاصة بكافة عمليات تأمين وجود البنك وتعاملاته على شبكة الإنترنت.

أيضا عالج القانون الأمريكي الخاص بالمحافظة على سرية البيانات المالية (GLB act) التزام جهة التوثيق الإلكتروني بالمحافظة على سرية البيانات التي تتطلع عليها بمناسبة تقديم خدماتها للبنوك الإلكترونية وعملائها، بل وفرض عليها أن تزود البنك وعملاءه بكافة التعليمات التي يجب عليهم الالتزام بها للمحافظة على سرية البيانات في البيئة الإلكترونية، وأن يتم تجديد وتطوير هذه التعليمات بما يتناسب مع المستجدات التي تطرأ على التعامل عبر شبكة الإنترنت[1].

نص أيضا القانون الصيني الخاص بطرق إدارة خدمات التوثيق الإلكتروني الصيني[2] "بالتزام جهة التوثيق الإلكتروني بالمحافظة على سرية البيانات الخاصة بخدمات التوثيق الإلكتروني".

وقد نص على هذا الالتزام أيضا المشرع التونسي في الفصل (١٥) من القانون رقم ٨٣ لسنة ٢٠٠٠ بشأن المبادلات والتجارة الإلكترونية بأن "على

---

required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community).

(1) **William Gram**, Legal; Op. Cit. p. 9.

David L. Baumer and others: Op. Cit, p. 404.

(٢) هذا القانون متاح على الموقع التالي:

www.japanpkiforum.jp/shiryou/sankou/CN_ecert_rule_E.pdf

مزودي خدمات المصادقة الإلكترونية، وأعوانهم المحافظة على سرية المعلومات التي عهد إليهم بها أثناء مباشرتهم لأنشطتهم، باستثناء تلك المعلومات التي يسمح صاحبها – كتابيا أو الكترونيا بنشرها، أو الإعلام عنها، أو في الحالات المنصوص عليها في التشريع الجاري العمل به".

ويلاحظ من خلال تدقيق النظر في هذا النص خاصة عبارة "المحافظة على سرية المعلومات التي عهد إليهم بها أثناء مباشرتهم لأنشطتهم "أن القانون التونسي قد استعمل عبارة عامة لفرض الالتزام بالسرية على جهة التوثيق، حيث إن المسئولية عن السرية تشتمل على كل المعلومات التي عهد بها إلى جهة التوثيق سواء كانت هذه المعلومات خاصة بالصفقات الإلكترونية التي تتم، أو كانت خاصة بالأشخاص المعنيين بهذه الصفقات والخاصة بالتوقيع الإلكتروني أو نظم التشفير التي يستخدمونها. يضاف إلى ذلك أن الخطاب موجه لمزودي خدمات المصادقة وأعوانهم، أي يشمل العاملين لدى جهة التوثيق سواء من الفنيين أو الجهاز الإداري(١).

وإذا كانت كافة النصوص السابقة قد عالجت الالتزام بالسرية في مجال عمل جهة التوثيق بصورة عامة، فأنها تبدو لنا قد قصرت إذ لم تراع الطبيعة الخاصة للسر المصرفي؛ والذي يعد وبحق المحور الذي يرتكز عليه نشاط أي بنك، الأمر الذي كان يستدعى وجود نص خاص يراعى طبيعة هذا الأمر ويضع ضوابط محكمة ومسؤوليات مشددة على عاتق جهة التوثيق، خاصة عند النظر لطبيعة البيانات التي تطلع عليها هذه الجهة بحكم عملها في تأمين تعاملات البنك مع عملائه.

---

(١) د. عبد الفتاح بيومى حجازى، مرجع سابق، ص١٦٠.

لكن السؤال: هل تعد جهة التوثيق والعاملين لديها من المخاطبين بأحكام السر المصرفي على الرغم من أنهم ليسوا في عداد موظفي البنك؟

٣٢٣- الإجابة على هذا التساؤل تقتضي منا التعرض لمدى اعتبار البيانات التي تطلع عليها جهة التوثيق من قبيل الأسرار المصرفية، ثم بيان مدى اعتبار جهة التوثيق والعاملين لديها من المخاطبين بأحكام السر المصرفي من عدمه، وذلك على النحو التالي:

أولا: مدى اعتبار البيانات التي تطلع عليها جهة التوثيق من قبيل الأسرار المصرفية:

٣٢٤- بداية لا يوجد في النظام القانوني المصري نص خاص يعالج النطاق الموضوعي للسر المصرفي في نظام عمل البنوك العاملة عبر شبكة الإنترنت. لكن من خلال مطالعة ما جاء في القانون رقم ٨٨ لسنة ٢٠٠٣ الخاص بالبنك المركزي والجهاز المصرفي والنقد في الفقرة الأولى من المادة (٩٧) نجد أن المشرع نظم النطاق الموضوعي للسر المصرفي بصور عامة، حيث نص على أن " تكون جميع حسابات العملاء وودائعهم وأماناتهم وخزائنهم وكذلك المعاملات المتعلقة بها سرية......".

ومن خلال تدقيق النظر فيما تطلع عليه جهة التوثيق من بيانات أثناء تقديم خدماتها للبنك وعملائه، نلاحظ أن هناك طريقين للاطلاع:

الأول: طريق مباشر، وذلك أثناء إصدار شهادة التوثيق، حيث تحصل جهة التوثيق على البيانات الشخصية للعميل، كما تزوده ببعض البيانات اللازمة لتأمين تعامله مع البنك، كالمفتاح الخاص بعملية التشفير، وكلمة المرور للدخول على

موقع البنك.

ومن خلال النظر في طبيعة البيانات التي تطلع عليها جهة التوثيق في الحالة الأولى، نلاحظ أن هذه البيانات لا تدخل ضمن النطاق الموضوعي للسر المصرفي كما عالجه المشرع المصري في النص سالف الذكر، مع العلم بأن هذا الموقف منتقد من قبل بعض الفقه[1]، الذي يرى اعتبار البيانات الشخصية للعميل من قبيل البيانات التي يجب أن يشملها السر المصرفي، وخاصة أن هذا الفقه يرى أن ما جاء في نص المادة (٩٧) سالفة الذكر هو تعداد موضوعي على سبيل المثال وليس الحصر، وذلك حتى يشمل ما قد يستجد من عمليات مصرفية في المستقبل وما تقتضيه من تعاملات. ونحن نؤيد هذا الفقه فيما ذهب إليه؛ حيث إن طبيعة المعاملات المصرفية على شبكة الإنترنت تتم باستخدام وسيلة إلكترونية عن بعد؛ الأمر الذي يعظم من أهمية البيانات الشخصية التي يستخدمها العميل في التواصل مع البنك عن بعد، ويجعلها بمثابة الوسائل التي لا غنى عنها لتعامل العميل مع البنك، والتي لا يجوز أن يعلمها سوى العميل، والتي يجب عليه أن يبلغ البنك عن أية سرقة تقع عليها من قبل الغير، الأمر الذي يجعل هذه البيانات من قبيل الأسرار المصرفية.

الثاني: طريق غير مباشر، والذي يظهر بحكم عمل جهة التوثيق كجهة مسئولة عن تأمين وجود البنك وتعاملاته المصرفية على شبكة الإنترنت، الأمر الذي يحتمل معه اطلاعها ولو بطريقة غير مقصودة على بعض البيانات المصرفية.

وبناء عليه تعد البيانات التي تطلع عليها جهة التوثيق أثناء تقديم خدمات التأمين

---

(١) د. **محي الدين إسماعيل علم الدين**. مرجع سابق، ص١١٧؛ **محمد عبد الحي حجازي**. مرجع سابق، ص١١٧.

للبنك وعملائه من قبيل الأسرار المصرفية.

ثانيا: مدى التزام جهة التوثيق بأحكام السر المصرفي:

٣٢٥- على الرغم من خلو القانون المصري من نص خاص ينظم التزام جهة التوثيق بالسر المصرفي، إلا أن ذلك لا يمنع من القول بأنها مخاطبة بأحكام المحافظة عليه وفقا لأحكام هذا القانون، وذلك لسببين:

١- أن المشرع المصري في مجال المعاملات المصرفية قد فرض الالتزام بالسرية المصرفية على غير العاملين لدى البنك، الذين يطلعون بحكم وظيفتهم على معلومات خاصة بحسابات العملاء سواء بطريق مباشر أو غير مباشر. حيث نص في الفقرة الأخيرة من المادة (٩٧) من قانون البنك المركزي رقم ٨٨ لسنة ٢٠٠٣ على أن "يسرى الحظر المنصوص عليه في الفقرة السابقة على جميع الأشخاص والجهات بما في ذلك الأشخاص والجهات التي يخولها القانون سلطة الاطلاع أو الحصول على الأوراق أو البيانات المحظور إفشاء سريتها طبقا لأحكام هذا القانون، ويظل هذا الحظر قائما حتى ولو انتهت العلاقة بين العميل والبنك لأي سبب من الأسباب".

وبناءً عليه يمتد هذا الحظر ليشمل جهة التوثيق الإلكتروني والعاملين لديها، حيث أنهم قد توافر في حقهم ذات العلة المقررة لموظفي البنك المركزي والجهاز المركزي للمحاسبات من كونهم يطلعون على هذه البيانات بحكم وظيفتهم وعملهم.

٢- أن قواعد العدالة والمنطق تفرض هذا الالتزام حتى ولو لم يوجد نص خاص بجهة التوثيق ينص صراحة على التزامها بالسرية المصرفية. فالأصل هو

حظر الاطلاع على مثل هذه البيانات، ولكن هناك ضرورة تدعو إلى الخروج على مثل هذا الحظر والسماح لجهة التوثيق بالاطلاع للتأكد من شخصية العميل، والضرورة تقدر بقدرها، أي يتم السماح لهم بالاطلاع مع التقيد بالمحافظة على السرية.

وفى كافة الأحوال، يجب أن يشدد البنك الإلكتروني أثناء تعاقده مع جهة التوثيق على ضرورة التزام جهة التوثيق باحترام سرية البيانات الخاصة بكل أنشطة التوثيق التي تطلع عليها جهة التوثيق بحكم عملها، وأن يشدد من مسؤولية جهة التوثيق عن الإخلال بهذا الأمر.

٣) ضمان سلامة البيانات الخاصة بتعاملات البنك الإلكتروني والعميل:

٣٢٦- ويقصد بهذا الالتزام تعهد جهة التوثيق بوضع المعايير الكفيلة بالحفاظ على سلامة وتكاملية البيانات المتبادلة بين البنك الإلكتروني والعميل ضد محاولات التعديل والتحريف[١].

فإذا كانت جهة التوثيق ملتزمة أصلا بالحفاظ على سرية البيانات، من خلال ضمان عدم الاطلاع عليها من قبل الأشخاص غير المخول لهم بهذا، فأن الالتزام بالسلامة يقتضى عدم المساس بهذه البيانات بأي وسيلة تستهدف تعديلها أو تغييرها، سواء من قبل أشخاص مخول لهم الاطلاع عليها أو غير مخول لهم بذلك، بالإضافة إلى الاعتماد على أجهزة موثقة ومؤمنة تكفل سلامة هذه البيانات.

والملاحظ على موقف المشرع المصري أنه لم يفرد نصا خاصا ينظم فيه

---

(1) **David L. Baumer and others**: Op. Cit, p. 407.

التزام جهة التوثيق بضمان سلامة المعلومات المتبادلة بين البنك الإلكتروني والعملاء؛ لذلك يجب على البنك الإلكتروني أن يورد هذا الشرط في العقد، وأن يشدد من مسؤولية جهة التوثيق عنه. وعلى فرض أن العقد جاء يخلو من مثل هذا النص، فإن جهة التوثيق تظل ملتزمة بهذا الالتزام وفقا للقواعد العامة، تلك التي تقضي بأن أطراف العقد لا يلتزمون فقط بتنفيذ العقد بنصوصه بطريقة تتفق مع مقتضيات حسن النية، ولكن أيضا بما هو من مستلزماته وفقا لما تقضي به قواعد القانون والعرف والعدالة حسب طبيعة الإلتزام (المادة ١٤٨ القانون المدني المصري). ولما كان التزام جهة التوثيق يدور حول توفير بيئة أمنة للبنك الإلكتروني على شبكة الإنترنت، فإن من مستلزماته وفقا لما تقضي به قواعد القانون والعرف والعدالة التزام جهة التوثيق بضمان سلامة المعلومات المتبادلة بين البنك الإلكتروني والعملاء.

هذا وقد جاء في كراسة شروط ومتطلبات منح تراخيص تقديم خدمات التوقيع الإلكتروني الصادرة عن هيئة تنمية صناعة تكنولوجيا المعلومات أن على الجهة طالبة الترخيص أن تستخدم نظام لتأمين المعلومات وحماية البيانات وخصوصيتها بمستوى حماية معين حددته الكراسة(١).

وكان الأجدر بالمشرع المصري، عند إصداره لقانون التوقيع الإلكتروني، أن يحرص على هذا الالتزام، وعدم الاكتفاء بصياغته من قبل هيئة تكنولوجيا المعلومات في كراسة الشروط الصادرة عنها؛ وذلك بالنظر إلى أهميته الكبرى،

---

(١) انظر **كراسة شروط ومتطلبات منح تراخيص تقديم خدمات التوقيع الإلكتروني** الصادرة عن هيئة تنمية صناعة تكنولوجيا المعلومات، الشروط والمواصفات الفنية (الأنظمة والقواعد مادة ٢ فقرة ١)، مرجع سابق، ص١٣.

خاصة في المعاملات المصرفية التي تتم عبر شبكة الإنترنت، وما تشكله قيمة البيانات وسلامتها من أهمية قصوى يتوقف عليها نجاح هذه المعاملات من عدمه. فالنص على هذا الالتزام من قبل جهة الترخيص يجعل الرقابة على توافره من سلطتها، الأمر الذي يمكن معه التهاون في استيفاء توافر هذا الشرط، وذلك على عكس الحال إذا كان القانون هو مصدر الإلزام؛ حيث تكون جهة التوثيق ملتزمة بهذا الالتزام في مواجهة البنك تحت رقابة القضاء.

وقد نص التوجيه الأوربي الخاص بالتوقيع الإلكتروني الصادر في ١٣ ديسمبر ١٩٩٩[(١)] على هذا الالتزام، حيث نص على ضرورة التزام جهة التوثيق بتوفير الوسائل التي من شأنها أن تضفى مزيدا من الحماية والثقة والأمان في التعامل، كما أوجب عليها قبل إصدار شهادات التصديق الإلكتروني أن تتحقق بالوسائل التقنية الملائمة من هوية الموقع وصفة الشخص الذي تقوم بتسليم الشهادة إليه، ويجب على جهة التوثيق أيضا أن تضمن عدم التلاعب بهذه البيانات، وأن تتخذ الاحتياطات الفنية التي من شأنها ضمان عدم تزوير الشهادات التي تصدرها.

أيضا تعرض قانون الأمم المتحدة النموذجي للتوقيع الإلكتروني الصادر في

---

(1) **Directive** EC, 1999/93/, Official Journal of the European Communities, Annex II (Requirements for certification- service- providers issuing qualified certificates), Official Journal of the European Communities item(f):

(Use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them)

٢٠٠١[١] في المادة العاشرة منه لهذا الالتزام، حيث نص علــى التــزام جهــة التوثيق باستخدام أشخاص ونظم معلوماتية جديرة بالثقة أثناء تقديم خدماتها، وهو ما يتطلب جودة المعدات ونظم المعلومات المستخدمة من قبل جهة التوثيق، كما يجب عليها أيضا أن تقوم بمراجعة هذه الوسائل بصورة مستمرة للتأكد من مدى كفاءتها.

وقد نص القانون السنغافوري[٢] أيضا على هذا الالتزام حيث جاء في المادة ٢٧ منه النص على "التزام جهــة التوثيــق باســتعمال نظــام جــدير بالثقــة Trustworthy system عند تقديم خدماتها". وقد بين ذات القــانون المقــصود بالنظام الجدير بالثقة بأنه النظام الذي يشتمل على مجموعة من الأجهزة والبرامج والإجراءات المسئولة عن الأمن ضد عمليــات التــدخل Intrusion، وإســاءة الاستخدام، ويقدم مــستوى معقــولا مــن الإتاحــة (Availability) والثقــة (Reliability)، والأداء المناسب للوظائف، والالتزام بإجراءات الأمن عموما.

هذا وقد وضع القانون السنغافوري[٣] قرينة بسيطة لمصلحة جهة التوثيــق

---

(1) (For the purposes of article 9, paragraph 1 (f), of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:

(b) Quality of hardware and software systems)

UNCITRAL Model Law on Electronic Signatures, Guide to Enactment, united Nations, 2001. p 1 available at:
www.unCitral.org/**pdf**/english/texts/electcom/ml-elecsig-e.**pdf**

(2) **Electronic Transactions ACT 1998**, Legal Guide to the Electronic Transactions, part VIII, (Duties of certification authorities).

(3) **Electronic transaction** ACT, Legal guide to the electronic transac-

تفيد بأنه منذ لحظة اتخاذ الإجراءات الأمنية اللازمة لتأمين السجل الإلكتروني يفترض أنه لم يعدل إلى أن يثبت العكس. بمعنى أنه إذا ثبت أن جهة التوثيق قد قامت بكل ما يلزم من إجراءات الأمن، فأنه على من يدعى حدوث تعديل في المستند الإلكتروني أن يثبت خطأ جهة التوثيق.

ونص القانون السنغافوري أيضا في ذات المادة على أن أي صفقة تتم باستعمال توقيع إلكتروني مؤمن فإنه يفترض إلى أن يثبت العكس أن:

- التوقيع الإلكتروني صادر عن صاحبه.
- التوقيع الإلكتروني تم من قبل صاحبه بنية الموافقة والتأكيد على التصرف القانوني الذي تم استعمال التوقيع بمناسبته.

ويبدو لنا أن مسلك المشرع السنغافوري في هذا الخصوص مسلك منتقد وذلك لسببين:

الأول: أن الصيغة المتبناة في هذا النص توحي بأن التزام جهة التوثيق بالمحافظة على سلامة البيانات الخاصة بعملية التوثيق هو مجرد التزام ببذل عناية، حيث يكفى أن تتخذ جهة التوثيق الإجراءات اللازمة لتأمين البيانات، الأمر الذي لا يتفق مع ما ينتظر من جهة التوثيق من جهد يتلاءم مع خطورة مباشرة العمليات المصرفية عبر شبكة الإنترنت وما تحتاجه من حرص وجهد أكبر يكون معه التزام جهة التوثيق بتحقيق نتيجة، بحيث يكون الخطأ مفترضًا في جانب جهة التوثيق وليس واجب الإثبات.

---

tions. chapter 88, Part v- 18.

الثاني: أن إلقاء عبء الإثبات على الطرف الضعيف في العلاقة، وهو الشخص الذي يحصل على خدمة التوثيق سواء كان البنك الإلكتروني أم العميل، من شأنه أن يثقل عليه على نحو يتعارض مع السياسة العامة التي تدعو إلى التشجيع على التعاملات الإلكترونية عبر شبكة الإنترنت بصورة عامة والتعامل مع البنوك الإلكترونية العاملة عليها بصورة خاصة في ظل قلة المعرفة الفنية بأمور الأجهزة والبرامج(١) ومن ثم صعوبة الإثبات.

ويتفرع عن الالتزام بضمان صحة المعلومات وحفظها عدة التزامات تقع على عاتق جهة التوثيق وتتمثل في:

أ- الاستعانة بأجهزة وبرامج فائقة:

٢٧٣- يجب على جهة التوثيق الاستعانة بأحدث الأجهزة والبرامج التي من شأنها توفير أكبر قدر ممكن من الأمن(٢)، فيجب أن تكون هذه الأجهزة حديثة، ومؤمنة بكافة الوسائل التي تمنع الغير من الشيء سرقة ما بها من البيانات المخزنة أو التلاعب فيها. ويقوم بجوار هذا الالتزام الحرص على ملاحقة التطور المستمر في مجال الحاسب ونظم المعلومات لضمان استمرارية تقديم الخدمة بشكل جيد(٣).

وقد نص على ذلك قانون طرق إدارة خدمات التوثيق الإلكتروني الصيني الصادر في فبراير ٢٠٠٥ في المادة الخامسة منه حيث "يجب على جهة التوثيق

---

(١) د. **جمال عبد الرحمن محمد على**، الخطأ في مجال المعلوماتية، (بدون دار نشر)، ٢٠٠٣، ص٦٥.

(٢) **William Gram**; Op. Cit, p. ٩.

(٣) د. **عبد الفتاح بيومى حجازى**،مرجع السابق، ص ٢١٠.

أن تمتلك الأجهزة والبرامج المناسبة، والتي تتوافق مع المعايير الأمنية الحكومية"

وكما سبق أن ذكرنا فإن على جهة التوثيق أن تزود عميل البنك بكافة الأجهزة والبرامج التي تلزم لتأمين تعاملاته مع البنك، ومن ثم فإنها مسئولة كذلك عن سلامة وأمان هذه الأجهزة في مواجهة البنك (باعتباره المشترط في مواجهة جهة التوثيق). كما أن البنك مسئول في مواجهة العميل عن سلامة وأمان هذه الأجهزة بحكم تعاقداته المصرفية مع العميل والتي يضمن البنك فيها سلامة وأمان الأجهزة بحكم ملكية البنك لهذه الأجهزة وتحظر على العميل أن يتصرف فيها(١).

ب- الاستعانة بالكفاءات البشرية المدربة:

٣٢٨- لا يكفى فقط الالتزام بتوفير الأجهزة والبرامج ذات الكفاءة العالية، ولكن يكمل هذا الالتزام ويتممه الالتزام من قبل جهة التوثيق بالاستعانة بالكفاءات البشرية المدربة والتي تتمتع بدرجة عالية من المهارة والخبرة التخصصية في تقنيات التشفير، والتوقيع الإلكتروني، وكافة إجراءات الأمن الصحيحة والمألوفة(٢). كذلك يجب أن يكون هؤلاء الأفراد موثوقًا بهم حتى لا يقوموا باستغلال البيانات التي بين أيديهم على نحو سيء(٣).

---

(١) (The equipment shall at all times remain the property of the Bank and the Customer shall not in any circumstances obtain any rights over, or in, the same).
MCB INTERNET BANKING, available at:
http://www.mcb.mu/documents/terms/ibterms.html

(٢) **محمد سعيد أحمد إسماعيل**، مرجع سابق، ص ٢٠٢.

(٣) المرجع السابق، ص ٢١١.

هذا وقد جاء في كراسة شروط ومتطلبات منح تراخيص تقديم خدمات التوقيع الإلكتروني الصادرة عن هيئة تنمية صناعة تكنولوجيا المعلومات في مصر، ما يفيد إلزام جهة التوثيق بالاستعانة بالمتخصصين من ذوى الخبرة الحاصلين على المؤهلات الضرورية لأداء الخدمات المرخص بها[١].

وقد جاء في الملحق الثاني من التوجيه الأوروبي[٢] سابق الإشارة إليه فقرة E أنه "يجب على مقدمي خدمة المصادقة الاستعانة بعاملين لديهم معرفة وخبرة بالخدمات المقدمة، وخاصة الكفاءة على المستوى الإداري، والخبرة في تكنولوجيا التوقيع الإلكتروني، والمعرفة التامة بإجراءات الأمن، حيث يجب عليهم تطبيق الإجراءات الإدارية والتنظيمية الكافية وفق المعايير المعترف بها".

٤) التزام جهة التوثيق بإصدار شهادات التوثيق لعملاء البنك الإلكتروني:

٣٢٩- يعتبر التزام جهة التوثيق بإصدار شهادات التوثيق لمن يرغب في التعامل مع البنك من أهم الالتزامات الملقاة على عاتقها في مواجهة البنك، الأمر الذي يقتضى تسليط مزيد من الضوء على هذا الالتزام، وذلك على التفصيل التالي:

---

(١) راجع العنوان الإلكتروني التالي: http://www.e-signature.gov.eg/guide.asp

(٢) **Directive** ١٩٩٩/٩٣/EC, ANNEX ١, Requirements for qualified certificates, Official Journal of the European Communities, item (e): (employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognized standards)

أ- أهمية شهادة التوثيق في نظام عمل البنك على شبكة الإنترنت:

٣٣٠- تتمتع هذه الشهادة بأهمية كبيرة في المعاملات التي تتم عبر شبكة الإنترنت بصورة عامة. ومبعث هذه الأهمية طبيعة الدور الذي تلعبه هذه الشهادات في دعم الثقة بين المتعاقدين عبر شبكة الإنترنت؛ وذلك من خلال التثبت من صحة التوقيع الإلكتروني، والتثبت من صحة البيانات الخاصة بهم (والتي تشتمل عليها الشهادة) ونسبتها إليهم(١).

لكن تحتل هذه الشهادة في نظام عمل البنك العامل عبر شبكة الإنترنت أهمية خاصة، وذلك للأسباب التالية:

- يتطلب الحصول على الخدمات المصرفية عبر شبكة الإنترنت الاستعانة بإجراءات أمنية مشددة؛ نظرا لما يترتب على هذا التعامل من السماح لعميل البنك من النفاذ إلى بياناته وحساباته المالية، الأمر الذي يتطلب ضرورة التزام جهة التوثيق بإصدار شهادات على درجة عالية من الدقة والموثوقية، بحيث تضمن إجراء المعاملة المصرفية بصورة أمنة(٢).
- تؤكد العديد من الدراسات القانونية على تزايد فرص وقوع جرائم غسيل الأموال عبر البنوك العاملة على شبكة الإنترنت؛ بفضل ما تتمتع به هذه

---

(١) **Thomas C. Glaessner and others**; Op. Cit. p. ٧١; **William Gram**; Op. Cit, p. ٥.

د. إسماعيل شاهين، مرجع سابق، ص٧؛د. إبراهيم الدسوقي أبو الليل، مرجع سابق، ص١٨٥٣.

(٢) د. عبد الفتاح بيومي حجازي،مرجع السابق، ص ٤٥٤؛

Apostolos Ath. Gkoutzinis; Op, Cit. p. ٢٢٢.

البنوك من إجراء عملياتها بصورة سريعة وعلى نطاق دول العالم بأسره، الأمر الذي دفع بهذه الدراسات إلى تأكيد أهمية شهادة التوثيق في نقل صورة مفصلة عن العميل، ليس فقط في ضوء بياناته الشخصية، ولكن أيضا بياناته المالية، ومدى مشروعية الأموال التي يتعامل بها مع البنك(١).

- نضيف إلى ذلك جانب آخر من الأهمية الخاصة لهذه الشهادات في نظام عمل البنك وهي أهمية الاعتبار الشخصي لعميل البنك، والذي قد يصعب على البنك التأكد من توافره في ظل التعامل عن بعد، الأمر الذي يبرز دور جهة التوثيق في التأكد من ذلك، وتضمين شهادة التوثيق لكافة البيانات التي تعرف البنك على شخصية عميله.

وانطلاقا من هذه الأهمية فقد حرصت العديد من التشريعات ورجال الفقه القانوني على وضع تعريف لهذه الشهادات؛ توضح فيه ماهيتها، والبيانات التي يجب أن تتوافر فيها، الأمر الذي يدعو إلى التعرض لهذا التنظيم، والنظر في مدى ملاءمته لنظام عمل البنوك على شبكة الإنترنت، وذلك على النحو التالي:

ب- تعريف شهادات التوثيق في نظام عمل البنك الإلكتروني:

٣٣١- تعددت التعريفات التى عالجت شهادادات التوثيق إلى تعريفات تشريعية وتعريفات فقهية، وذلك على التفصيل التالى:

- التعريف التشريعي:

---

(١) Ibid, p. ١٨٩.

عرفت شهادة التوثيق في قانون التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤ في المادة (١/ و) بأنها عبارة عن "شهادة تصدر من الجهة المرخص لها بالتصديق، تثبت الارتباط بين الموقع وبيانات إنشاء التوقيع"(١).

عرفت أيضا في المادة ٢/٩ من التوجيه الأوروبي رقم ٩٩-٩٣ لعام ١٩٩٩ بأنها عبارة عن "شهادة إلكترونية تربط بيانات التوقيع بشخص ما وتؤكد هوية ذلك الشخص"(٢).

عرفت كذلك في الفصل الثاني من القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية رقم ٨٣ لسنة ٢٠٠٠ بأنها عبارة عن "الوثيقة الإلكترونية المؤمنة بواسطة الإمضاء الإلكتروني للشخص الذي أصدرها والذي يشهد من خلالها أثر المعاينة، على صحة البيانات التي تتضمنها".

عرفها قانون الأونيسترال الخاص بالتوقيع الإلكتروني ٢٠٠١ بأنها عبارة عن رسالة بيانات أو أي سجل آخر يؤكد الارتباط بين الموقع وبيانات إنشاء التوقيع"(٣).

وعرفت أيضا في المادة الثانية من الفصل الأول من القانون الخاص بالمعاملات والتجارة الإلكترونية لدولة الإمارات العربية المتحدة رقم (٢) لسنة

---

(١) هذا القانون متاح على العنوان التالي:
http://www.isdo.gov.eg/Esignature-law-text.asp

(٢) **Directive** ١٩٩٩/٩٣/EC, A community framework for electronic signatures, Official Journal of the European ١٩١. ٢٠٠٠, p. ١٤.

(٣) هذا القانون متاح على الموقع التالي:
www.unCitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

٢٠٠٢ بأنها عبارة عن "شهادة يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معينة".

والملاحظ على جميع هذه التعريفات أنها عرفت شهادة التوثيق للمعاملات التي تتم عبر شبكة الإنترنت بصورة عامة، ولم تراع خصوصية المعاملات المصرفية عبر هذه الشبكة، الأمر الذي يعكس قصورا في هذه التشريعات.

- **التعريف الفقهي:**

عرفت شهادة التوثيق من قبل جانب من الفقه[١] بأنها عبارة عن "صك أمان يفيد صحة وضمان المعاملة الإلكترونية من حيث صحة البيانات ومضمون المعاملة".

وعرفها جانب آخر[٢] بأنها عبارة عن "شهادات تفيد صحة التصرف ونسبته إلى من صدر عنه".

وعرفت أيضا بأنها عبارة عن "شهادة تصدر عن طرف ثالث موثوق به (Trusted third parties) تحدد هوية المتعاملين وتشهد بصحة التوقيع الإلكتروني".[٣]

ويلاحظ على جميع التعريفات السابقة أنها عرفت شهادة التوثيق بصورة عامة، ولم تفرد تعريفا خاصا لشهادة التوثيق الخاصة بالتعامل المصرفي عبر شبكة

---

(١) د. **عبد الفتاح بيومى حجازي**،مرجع السابق، ص ٤٥٤.

(٢) د. **سمير حامد الجمال**، المرجع السابق، ص ٣٢١.

E-Banking; Op. Cit, p. ٧; **Marie Wright**; Op. Cit, p. ١٠; **William Gram**; Op. Cit, p. ٥.

(٣) **Apostolos Ath. Gkoutzinis**; Op, Cit, p. ١٨٧.

الإنترنت، على نحو يبرز خصوصية هذه الشهادة.

ويبدو لنا أن نعرف شهادة التوثيق الخاصة بالتعامل المصرفي عبر شبكة الإنترنت بأنه عبارة عن صك إلكتروني تمنحه جهة توثيق معتمدة يشتمل على كافة البيانات الخاصة بالمتعامل مع البنك، وتشهد بأهليته لهذا التعامل، وتضمن صحة التصرفات القانونية الصادرة عنه وتثبتها.

ت) البيانات الواجب توافرها في شهادة التوثيق:

٣٣٢- وعن البيانات التي يجب أن تتوافر في شهادة التوثيق الإلكتروني، فقد خلا قانون التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤ من عرض لهذه البيانات، واكتفى بمجرد الإحالة إلى اللائحة التنفيذية لهذا القانون، حيث نص في المادة (٢٠) منه على أنه يجب أن تشتمل شهادة التصديق الإلكتروني على البيانات التي تحددها اللائحة التنفيذية لقانون التوقيع الإلكتروني.

هذا وقد عرض التوجيه الأوربي الخاص بالتوقيع الإلكتروني لهذه البيانات على النحو التالى(١):

أ- هوية من صدرت له الشهادة.

ب- هوية مقدم خدمة التوثيق الإلكتروني والدولة التي رخصت له بمباشرة نشاطه.

---

(١) **Directive** ١٩٩٩/٩٣/EC, ANNEX ١, Requirements for qualified certificates, Official Journal of the European Communities, p. ١٨.
انظر أيضا: في عرض هذه البيانات قانون الأونيسترال النموذجي الخاص بالتوقيعات الإلكترونية ٢٠٠١ في المادة التاسعة.

ج- بيانات التوقيع الحقيقي أو المستعار مادام يؤدى إلى التحقق من هوية هذا الموقع.

د- إذا كان هناك أي علامة أو خاصية مميزة لصاحب التوقيع مرتبطة بالغرض الذي من أجله صدرت الشهادة.

ه- بيانات إثبات التوقيع التي تتطابق مع بيانات إنشاء التوقيع.

و- تحديد تاريخ بداية ونهاية صلاحية شهادة التوثيق.

ز- الرمز الخاص بالشهادة.

ح- التوقيع الرقمي الخاص بجهة التوثيق التي أصدرت الشهادة.

ط- نطاق استعمال الشهادة، أن أمكن.

ي- قيمة الصفقات التي يمكن أن تستخدم فيها الشهادة.

وعلى صعيد التشريعات العربية(١)، فقد نظم القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية أيضا هذه البيانات في الفصل السابع عشر منه حيث جاء فيه: "يصدر مزود خدمات المصادقة الإلكترونية شهادات مصادقة تستجيب لمقتضيات السلامة والوثوق بها. وتضبط المعطيات التقنية المتعلقة بالشهادة والوثوق بها بقرار من الوزير المكلف بالاتصالات، وتتضمن هذه الشهادة بالخصوص:

أ- هوية صاحب الشهادة.

---

(١) أيضا المادة (٢٤) بند (٣) من القانون الإماراتي رقم ٢ لسنة ٢٠٠٢ بشأن المعاملات والتجارة الإلكترونية.

ب- هوية الشخص الذي أصدرها وإمضاءه الإلكتروني.

ج- عناصر التدقيق في إمضاء صاحب الشهادة.

د- مدة صلاحية الشهادة.

ه- مجالات استعمال الشهادة.

والملاحظ على هذه القوانين أنها عددت مجموعة من البيانات للتعريف بشخصية من صدرت له الشهادة، وهي بيانات تمثل ما يجب معرفته عن العميل بصدد أي معاملة إلكترونية تتم عن بعد. كما أنها راعت الطبيعة الخاصة للمعاملات المصرفية، ومدى أهمية الاعتبار الشخصي للعميل في هذه المعاملات؛ وما يتطلبه ذلك من رغبة في التعرف على الضمانات المالية للعميل، للنظر في مدى أهليته للحصول على الخدمات المصرفية في ضوء حجم ونوعية هذه الضمانات. فقد جاء البند (ى) من التوجيه الأوربي سالف الذكر متطلبًا "بيان قيمة الصفقات التي يمكن أن تستخدم فيها الشهادة"، وأيضا القانون التونسي البند (ه) تطلب ذكر "بيان بمجالات استعمال الشهادة". وما من شك في أهمية توضيح مثل هذه البيانات في شهادة التوثيق، وذلك لنقل رؤية واضحة للبنك عن العميل وحالته المالية، حيث سيحرص البنك على ربط حجم ونوعية الخدمات المصرفية التي يقدمها للعميل في ضوء ملاءته المالية التي تفصح عنها شهادة التوثيق(١).

ث) إجراءات إصدار شهادة توثيق للتعامل مع البنك الإلكتروني:

٣٣٣- تبدو أهمية ذكر إجراءات إصدار شهادة توثيق للتعامل مع البنك في

(١) **David L. Baumer and others**; Op. Cit, p. ٤٠٣.

إبراز الواجبات التي تلتزم بها جهة التوثيق في مواجهة البنك ومن يريد التعامل معه، وأيضا إعلام الأخير بالخطوات التي يجب عليه اتباعها للتأكد من حقيقة موقع البنك وأنه ليس مجرد موقع وهمي، ثم الحصول على الشهادة التي تمكنه من التعامل مع البنك عبر شبكة الإنترنت.

وتبدأ هذه الإجراءات بقيام البنك بالتعاقد مع إحدى جهات التوثيق الإلكتروني على إصدار شهادات توثيق للبنك الإلكتروني وعملائه، وبموجب هذا التعاقد تقوم جهة التوثيق بإصدار شهادة توثيق خاصة بالبنك الإلكتروني، والتي تشتمل على البيانات الخاصة بالبنك، وعلى المفتاح العام الخاص به والمرتبط بالمفاتيح الخاصة بالعملاء، كما تحتوى الشهادة على تاريخ انتهاء سريانها، وكذلك على بيانات عن تصريح الممارسة (CPS)(١).

ويتضمن هذا العقد ما يفيد التزام جهة التوثيق بإصدار شهادة توثيق لمن يريد التعامل مع البنك لصالح البنك.

وتمر إجراءات إصدار شهادة توثيق لمن يريد التعامل مع البنك بمجموعة من الخطوات على النحو التالي(٢):

---

(١) (cps) هي اختصار لـ (Certification Practice Statement) وهي عبارة عن بيان يصدر عن السلطة المختصة يوضح اختصاصات وصلاحيات جهة التوثيق في إصدار شهادات التوثيق. انظر:

Legal guide to the electronic transactions ACT, Singapore, part ١-preliminary, p. ٥.

(٢) **محمد سعيد أحمد إسماعيل**، المرجع السابق، ص٢٠٨ وما بعدها؛ انظر أيضا: **رأفت رضوان**، مرجع السابق، ص٩٨ وما بعدها.

Alain Hiltgen. Thorsten kramp. Thomas, Op, Cit, p. ٢٩; **Authentication in an Electronic Banking Environment**, Op. Cit,

(أ) يقوم الشخص الذي يرغب في الحصول على شهادة توثيق إلكتروني بالاتصال بجهة التوثيق المتعاقد معها البنك[١] لطلب شهادة توثيق إلكتروني لمفتاحه العام الذي حصل عليه من البنك (والذي يرتبط بالمفتاح الخاص بالبنك الإلكتروني) حيث يقوم بتقديم الأوراق التي تثبت شخصيته (كبطاقته الشخصية، جواز السفر، وغيرها من المستندات التي تفيد جهة التوثيق في ذلك)، تقوم جهة التوثيق بعد أن تتأكد من هذه البيانات بإصدار شهادة توثيق خاصة بهذا العميل، والتي تشتمل على المفتاح العام (public key) الخاص به، ويحصل على رمز، أو علامة للتسجيل (Token registered) يستعمله عند التعامل مع البنك الإلكتروني[٢]، وقبل أن تسلم جهة التوثيق هذه الشهادة للعميل تقوم بالتوقيع على هذه الشهادة بمفتاحها الخاص والذي يسمى المفتاح الجذري (Root key)، حيث إن هذا التوقيع من شأنه إضفاء الرسمية على

---

p. ٩;-**A. Michael Froomkin**; Op. Cit, p. ٦; **William Gram**; Op. Cit, p. ١١.

(١) ويجب على البنك أن يشير بوضوح إلى جهة التوثيق المتعاقد معها على موقعه الإلكتروني حتى يسهل على من يريد الحصول على شهادة توثيق الاتصال بهذه الجهة. وهذا وقد أشارت التوجيهات الأوربية(٢٠٠٢/٢٠١٣) إلى مجموعة من البيانات التي يجب أن يلتزم بها من يتعامل على شبكة الانترنت بإعلام عملائه بها، وهذه البيانات تدور حول فكرة توجيه العميل للخطوات اللازمة للتعاقد، وتعد إشارة البنك لجهة التوثيق والخطوات التي يجب على العميل اتباعها من ضمن هذه البيانات.

Goodwin, Procter& Hoar LLp, Op, Cit, p. ٢; **Apostolos Ath. Gkoutzinis**; Op, Cit, p. ١٨٤.

(٢) **Shirley Radack,** Electronic Authentication: guidance for selecting secure techniques, article available at: http://www.itl.nist.gov/lab/bulletns/bltnaug٠٤.htm

هذه الشهادة[1].

(ب) عندما يقدم العميل على التعامل مع البنك، فإنه يقوم بالدخول على موقعه الإلكتروني على شبكة الإنترنت، ثم يتحقق من وجود وصحة شهادة التوثيق الخاصة بالبنك من خلال الرجوع لقائمة الإلغاءات (Certification Revocation List) الموجودة لدى جهة التوثيق، وذلك للتأكد من أن صفحة الويب الخاصة بالبنك الإلكتروني حقيقية وشرعية. كذلك يتأكد من أن المفتاح العام للبنك ساري المفعول، وبعد أن يتأكد العميل من ذلك يستطيع أن يقوم بإرسال شهادة التوثيق الخاصة به والتي تعد بمثابة أوراق اعتماد إلكترونية (electronic credentials) لهذا العميل[2]، هذا بالإضافة إلى كافة البيانات الخاصة بالعملية المصرفية التي يريد الحصول عليها من البنك.

(ج) قبل أن يجيب البنك طلب العميل، يقوم بالتأكد من وجود وصحة شهادة هذا العميل، وذلك من خلال الاتصال بجهة التوثيق، فإذا تم له ذلك فإنه يتابع تنفيذ العملية المطلوبة مع هذا العميل.

ويعد تبنى البنك الإلكتروني لنظام شهادات التوثيق المعتمدة على نظام المفتاح العام (PKI) هو من أفضل طرق التعريف بشخصية العملاء، ليس هذا فحسب، ولكن أيضا من أفضل الطرق التي يمكن للعملاء الاعتماد عليها للتأكد من حقيقة موقع البنك الإلكتروني على شبكة الإنترنت[3].

---

(١) **M.Sklira. A.S.pomportsis. M.S. Obaidat**; Op. Cit, p. ١٧٨٠.

(٢) **Ibid,** p. ١٧٨٠.

(٣) **Alain Hiltgen. Thorsten kramp. Thomas**; Op, Cit, p. ٢٧.

ع) التزامات جهة التوثيق بخصوص شهادة توثيق عميل البنك:

٣٣٤- وهناك بعض الالتزامات التي تقع على عاتق جهة التوثيق عند إصدار شهادات التوثيق لصالح عملاء البنك الإلكتروني والتي تتمثل في الآتي[١]:

استخدام نظام موثوق به (Trustworthy System) لتقديم الخدمات المتعلقة بالشهادات.

٣٣٥- ويقصد بهذا الالتزام اعتماد جهة التوثيق على أدوات تقنية مجهزة ومؤمنة والاستعانة بالكفاءات البشرية المدربة، وإعلام العميل بكافة المعلومات اللازمة لاستخدام الشهادة، وذلك على التفصيل التالي:

أ- يجب على جهة التوثيق أن تتبنى نظم تقنية عالية الكفاءة، ومؤمنة ضد كافة أشكال التدخل غير المشروع الذي يستهدف بيانات الشهادة، سواء عند إصدارها أو إلغائها، وذلك من خلال الاستعانة بأحدث الأجهزة المخصصة لهذا الغرض، وتأمينها بنظم تشفير قوية بحيث تضمن أعلى مستوى من الدقة والكفاءة والتأمين عند تقديم خدمات الشهادات[٢].

ويجب على البنك أن يشدد على التزام جهة التوثيق بهذا الأمر، ويشدد من مسؤوليتها في هذا الخصوص، وذلك من خلال إلزام جهة التوثيق بمراعاة المعايير القياسية العالمية[٣] بحيث تراعى الطبيعة الخاصة للمعاملات المصرفية

---

(١) **Chris Reed**; Op. Cit, p. ١٥٧.

(٢) **William Gram**; Op. Cit, p. ١٣.

(٣) **د.ثروت عبد الحميد**، مرجع سابق، ص ١٦٣

وما تحتاج إليه من درجات عالية من التأمين والموثوقية[1].

ب- الاستعانة بمجموعة من العاملين المؤهلين أصحاب المعرفة التخصصية والخبرة الفنية بتقديم خدمات شهادات التوثيق، وما يرتبط بها من خدمات التوقيع الإلكتروني وتقنياته[2]. يضاف إلى ذلك التأكد من موثوقية هؤلاء العاملين والتشديد على التزامهم بسرية كافة البيانات التي يحصلون عليها ممن يريد التعامل مع البنك؛ خاصة أن هذا العميل قد يدلي ببعض البيانات الخاصة بمحتويات ذمته المالية (للدلالة على ملاءته المالية).

و نرى أن يلزم البنك جهة التوثيق بتخصيص بعض العاملين من أصحاب الخبرة في التعاملات المالية لإصدار الشهادات الخاصة بالبنك؛ بحيث يطالبون العميل بالإدلاء بالبيانات التي تفيد البنك في التعرف على شخصية العميل، وظروفه المالية، ومشروعية أمواله، وغيرها من البيانات التي يحتاج إليها البنك للتعرف على حقيقة وضع العميل.

ج- تلتزم جهة التوثيق بإعلام عميل البنك بكافة الإرشادات والتوجيهات الفنية والقانونية اللازمة لاستخدام الشهادة وتقنيات التوقيع الإلكتروني المرتبطة بها، بما في ذلك حالات الاستعمال وحدوده (قيمة الصفقات التي يمكن أن تستخدم فيها الشهادة)، وحالات الامتناع عن الاستعمال، بالإضافة إلى

---

(١)**William Gram**; Op. Cit, p. ١٨.

(٢)**Alain Hiltgen. Thorsten kramp. Thomas**, Op, Cit, p. ٢٩, **Authentication in an Electronic Banking Environment**, Op. Cit, p. ٩, **A. Michael Froomkin**; Op. Cit, p. ٦, **William Gram**; Op. Cit, p. ١١.

الاحتياطات الأمنية المرتبطة باستخدام الشهادة(١).

هذا وقد أولت التشريعات القانونية اهتماما خاصا بالتزام جهة التوثيق بالإعلام بالمفهوم السابق. ويبرر ذلك بالطبيعة الفنية المعقدة لاستخراج هذه الشهادات واستعمالها، الأمر الذي يجب معه إحاطة طالب شهادة التوثيق بالبيانات اللازمة لذلك.

وعن موقف القانون المصري في ذلك، فقد سكت قانون التوقيع الإلكتروني عن الحديث عن التزام جهة التوثيق بالإعلام. هذا وقد جاء في الأحكام العامة الواردة في العقد النموذجي (الموضوع من قبل هيئة تكنولوجيا صناعة المعلومات) الذي ينظم علاقة جهة التوثيق بطالب خدمات التوثيق (البنك العامل على شبكة الإنترنت)، تفصيلا لالتزام جهة التوثيق بالإعلام، وذلك على النحو التالي(٢):

- يجب على جهات إصدار شهادات التصديق الإلكتروني إحاطة طالب إصدار شهادة التوثيق بكافة الشروط والالتزامات التعاقدية، وذلك قبل التعاقد.

- يجب على جهات إصدار شهادات التصديق الإلكتروني إحاطة طالب إصدار شهادة التصديق بأية قيود مفروضة على استخدام الشهادة، واطلاعه على ما يفيد اعتماد جهة التصديق لدى هيئة تنمية صناعة تكنولوجيا المعلومات، كما يجب إحاطته علما بإجراءات الشكاوى وتسوية المنازعات، على أن يتم ذلك بلغة مفهومة وقابلة للقراءة من قبل حامل الشهادة.

---

(١) **Ibid**, p. ١٧.

(٢) راجع نموذج العقد على العنوان الإلكتروني التالي:
http://www.e-signature.gov.eg/guide.asp

وحسنا فعلت هيئة تكنولوجيا صناعة المعلومات فيما أوردته من نص يفرض على جهة التوثيق الالتزام بإعلام البنك العامل عبر شبكة الإنترنت، بالبيانات اللازمة للتعاقد مع جهة التوثيق، وأيضا البيانات اللازمة لاستخدام شهادة التوثيق. ولعل ما يبرر هذا الموقف؛ هو إدراك الهيئة لأهمية الالتزام بالإعلام في ظل التفاوت بين جهة التوثيق ومتلقي الخدمة (البنك وعملائه) في الإلمام بالجوانب المتعلقة باستخدام شهادة التوثيق، بما يفرض على الأولى إحاطة الثاني بكافة البيانات والإرشادات المتعلقة باستخدام الشهادة، سواء من الناحية القانونية أم الفنية.

وعلى الرغم من ذلك، فإن الالتزام بالإعلام يتمتع بأهمية كبيرة، وذلك على النحو الذي كان يجب معه معالجة هذا الالتزام صراحة من قبل المشرع بنص صريح في قانون التوقيع الإلكتروني، ولا يترك تنظيمه للشروط التعاقدية، حتى لا تستبعده جهة التوثيق تحت أي ظرف.

هذا وقد تضمن التوجيه الأوربي[1] هذا الالتزام، وأشار إلى ضرورة أن

---

(١) **Directive** ١٩٩٩/٩٣/EC, Annex II (Requirements for certification-service- providers issuing qualified certificates), Official Journal of the European Communities item(k)
(Before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to

يكون إعلام العميل بهذه الإرشادات بصورة مكتوبة حتى ولو بصورة الكترونية، وأن يكون باللغة التي يمكن للعميل أن يفهمها. بل أضاف إلى ذلك أن جهة التوثيق يجب أن تتيح الاطلاع على هذه الإرشادات للأشخاص الذين يعتمدون في التعامل مع العميل على هذه الشهادة.

وحسنا فعل المشرع الأوربي في هذا الخصوص نظرا لأهمية هذا الالتزام، خاصة إذا جاء العقد يخلو من بند يشير إليه صراحة.

أيضا في الولايات المتحدة الأمريكية تضمن المركز التجاري الفيدرالي **(Federal Trade Center)** هذا الالتزام، بل إنه ألزم جهة التوثيق بالإفصاح عن هذه الإرشادات للعميل قبل أن يدلي هو بالبيانات الخاصة به(١).

د- يجب على جهة التوثيق اتباع إجراءات مشددة لحفظ شهادات التوثيق والبيانات الخاصة بأصحابها، وذلك من خلال الاستعانة بأفضل الأجهزة والبرامج للتعامل مع هذه البيانات، وحظر الدخول على قواعد البيانات الخاصة بهذه الشهادات إلا من قبل الأشخاص المخول لهم ذلك(٢).

وتبدو أهمية هذا الالتزام في إمكانية الحاجة لهذه البيانات في حالة حدوث منازعة بين البنك وعمليه في خصوص أحد هذه البيانات، حيث ستكون المعلومات المحفوظة لدى جهة التوثيق هي المرجع الذي يعتمد عليه لفض هذه

---

third-parties relying on the certificate).

(١) **David L. Baumer and others**; Op. Cit, p. ٤٠٣.

(٢) **William Gram**; Op. Cit, p. ١٢;

Ben Moshinsky, Pay checks, the lawyer (centauer communication), ٩ October, ٢٠٠٦, p. ٣٢. available at: www.THELAWYER.com.

المنازعة، الأمر الذي يحتم على جهة التوثيق إعداد سجل إلكتروني لحفظ هـذه الشهادات وأن تتخذ كافة الإجراءات اللازمة لتأمينه.

هذا ولم ينظم قانون التوقيع الإلكتروني المصري هذا الالتزام، على الـرغم من أهميته القصوى. كما لم يرد بشأنه أية إشارة من قبل هيئة تنمية تكنولوجيـا صناعة المعلومات.

وعن موقف التشريعات الأخرى، فقد تـضمن التوجيـه الأوربـي(١) هـذا الالتزام، ولم يكتف بمجرد النص، بل صاغ الآلية التي يمكن من خلالها لجهـة التوثيق أن تتعامل مع هذه البيانات، والتي تتمثل في(٢):

- حظر الدخول على البيانات المحفوظة الخاصة بالبنك إلا من قبل الأشخاص المخول لهم بذلك فقط.
- الاطلاع على هذه البيانات يكون لأغراض التوثيق فقط.
- اطلاع الغير على هذه البيانات يكون بترخيص من العميل بذلك.

هذا وقد نظم القانون التونسي للمبادلات الإلكترونية هذا الالتزام، حيث نص في المادة ١٤ على أنه "على كل مزود خدمات المصادقة الالكترونية مسك سجل

---

(١)**Directive** ١٩٩٩/٩٣/EC, Annex II (Requirements for certification-service- providers issuing qualified certificates), item (i):
(Record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically)

(٢)**Directive** ١٩٩٩/٩٣/EC, Annex II (Requirements for certification-service- providers issuing qualified certificates), item (l)

الكتروني لشهادات المصادقة على ذمة المستعملين مفتوح للاطــلاع الكترونيــا بصفة مستمرة على المعلومات المدونة به. ويتضمن سجل شهادات المــصادقة، عند الاقتضاء، تاريخ تعليق الشهادات أو إلغاءها، ويتعين حماية هــذا الــسجل وشهادة المصادقة من كل تغيير غير مرخص به".

٢- التزام جهة التوثيق باتباع إجراءات دقيقة للحصول علــى البيانــات الخاصة بعميل البنك والتأكد من صحتها، وذلك قبل إصدار شهادة التوثيق له، والالتزام بعدم إدخال أي تعديلات أو إضافات على هذه البيانات.

٣٣٦- هذا وقد جاء قانون التوقيع الإلكتروني المصري خلوًا من نص ينظم التزام جهة التوثيق بجمع البيانات الخاصة بعميل البنك والتأكد من صحتها.

لكن التوجيه الأوربي (EC/١٩٩٩/٩٣)[1] لم يغفل عن هذا الأمر؛ حيــث ألزم جهة التوثيق، قبل إصدار الشهادة، بجمع المعلومات اللازمة لإصدار الشهادة مباشرة من طالب الشهادة، ولها أن تحصل عليها من قبل الغير بعــد الحــصول على الموافقة الكتابية من طالب الشهادة. كما حظر على جهة التوثيق جمع أيــة معلومات غير ضرورية لإصدار الــشهادة. وحظــر عليهــا أيــضا اســتعمال المعلومات التي تحصل عليها خارج نطاق عملية التوثيق، ما لم تحــصل مــن

---

(١) **Directive** ١٩٩٩/٩٣/EC, article ٨ (data protection),item ٢:
(Member States shall ensure that a certification-service provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.).

الطالب على موافقته الكتابية.

أيضا نظم القانون التونسي للمبادلات الإلكترونية هذا الالتزام[١] بصيغة مقاربة من تلك التي تبناها التوجيه الأوربي سالف الذكر.

ويتفرع عن الالتزام السابق التزام جهة التوثيق بضمان صحة البيانات الواردة في الشهادة وذلك من تاريخ تسليم الشهادة للبنك وعميله، كما تضمن أيضا الصلة بينهم وبين التوقيعات الخاصة بهم[٢].

وعلى الرغم من الأهمية القصوى التي يحتلها هذا الالتزام في علاقة جهة التوثيق بالبنك وعملائه، إلا أن المشرع المصري لم يتعرض لتنظيم هذا الالتزام أيضا، وأن كان مما يخفف من غلواء هذا القصور، ما جاءت به الأحكام العامة في العقد الذي يحكم علاقة جهة التوثيق بطالب خدمة التوثيق، حيث عرض لمسؤولية جهة التوثيق عن صحة البيانات الواردة في شهادة التوثيق، وذلك على النحو التالي:

تتحمل جهة التوثيق الإلكتروني المسؤولية القانونية عن الأضرار والخسائر التي تحدث لأي جهة أو شخص طبيعي أو معنوي نتيجة استخدامهم للشهادات

---

(١) انظر الفصل (١٦) من القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية رقم ٨٣ لسنة ٢٠٠٠.

(يتولى مزود خدمات المصادقة الإلكترونية، عند طلب شهادة جمع المعلومات ذات الصبغة الشخصية، مباشرة من الشخص المعني وله أن يتحصل عليها من الغير بعد الموافقة الكتابية أو الإلكترونية لهذا الشخص. يحجر (يحظر) على مزود خدمات المصادقة الإلكترونية جمع المعلومات التي لا تكون ضرورية لتسليم الشهادة ويحظر عليه استعمال المعلومات التي جمعها بغرض تسليم الشهادة خارج إطار انشطة المصادقة، ما لم يحصل كتابيا أو الكترونيا على موافقة الشخص المعني).

(٢) **William Gram**; Op. Cit, p. ١٣.

المصدرة، وذلك في الحالات التالية(١):

- عدم دقة تسجيل بيانات الشهادة، وقت إصدار الشهادة.
- عدم التأكد من أن الموقع يحمل المفتاح الشفري الخاص المناظر للمفتاح الشفري العام الموجود بالشهادة المصدرة.

وقد نص التوجيه الأوربي **أيضا** على مسؤولية جهة التوثيق عن ضمان صحة البيانات الواردة في شهادة التوثيق، وأنها المسئولة عن أية أضرار تلحق أي شخص طبيعي أو معنوي اعتمد على البيانات الواردة في هذه الشهادة. وأضاف "ما لم تثبت جهة التوثيق عدم صدور إهمال منها"(٢).

والملاحظ أن الصيغة التي جاءت في العقد الذي يحكم علاقة جهة التوثيق بطالب خدمة التوثيق، وتلك التي جاء بها التوجيه الأوربي متقاربة؛ فكلاهما أقر

---

(١) انظر نموذج طلب الترخيص (رقم ٢)، القواعد الحاكمة لإجراءات الحصول على الخدمة، البند الثامن (المسؤولية القانونية لطالب الترخيص)، متاح على العنوان الإلكتروني التالي:

http://www.itida.gov.eg.eg/csp.

وهذا ما نصت عليه أيضا العديد من التشريعات العربية، انظر الفصل (١٨)، الفصل (٢٢) من **القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية** رقم ٨٣ لسنة ٢٠٠٠. انظر أيضا: المادة (٢٤) بند (١) فقرة (ب) من **القانون الإماراتي** رقم ٢ لسنة ٢٠٠٢ بشأن المعاملات والتجارة الإلكترونية.

(٢) **Directive** ١٩٩٩/٩٣/EC, article ٦ (liability):

(As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate….unless the certification-service-provider proves that he has not acted negligently).

بالتزام جهة التوثيق بضمان صحة البيانات المدرجة في شهادة التوثيق. كما أن كلاً منهما أقر بمسؤولية هذه الجهة فقط في الحالات التي يثبت فيها خطأ جهة التوثيق.

ويبدو لنا أن هيئة تنمية تكنولوجيا المعلومات المصري والمشرع الأوربي قد حالفهما التوفيق في الجزء الأول؛ المتعلق بالنص على التزام جهة التوثيق بضمان صحة البيانات المدرجة في شهادة التوثيق، لكن هذا التوفيق قد تخلا عنهما، وذلك عندما قررا إعفاء جهة التوثيق من المسؤولية إذا ما تمكنت من إثبات عدم صدور خطأ أو إهمال عنها.

فأهمية الدور الذي تطلع به شهادة التوثيق في معاملات التجارة الإلكترونية بصورة عامة والمعاملات المصرفية على شبكة الإنترنت بصورة خاصة، تأبى أن تكون مسؤولية جهة التوثيق عن الأضرار التي تقع نتيجة عدم صحة البيانات الواردة فيها مجرد مسؤولية خطئية يجب لقيامها إثبات الخطأ، ويكفي لدفعها إثبات عدم ارتكاب الخطأ. فالأمر أخطر من ذلك؛ فالمعاملات المصرفية على شبكة الإنترنت تتم عن بعد، في ظل غياب مادي لأطراف العلاقة، يضاف إلى ذلك تعاظم فكرة الاعتبار الشخصي للعميل من وجهة نظر البنك، الأمر الذي يؤكد أهمية الدور الذي تلعبه شهادة التوثيق وصحة ما بها من بيانات، في الحد من مشاكل التعاقد عن بعد والتعريف بشخصية العميل، كل ذلك من شأنه أن يفرض ضرورة تبنى المسؤولية القائمة على فكرة المخاطر (تحمل التبعة) والتي تقضى بمسؤولية جهة التوثيق عن أي ضرر يلحق البنك نتيجة عدم صحة البيانات الواردة في شهادة التوثيق حتى ولو لم يثبت الخطأ من قبل جهة التوثيق، كما أن جهة التوثيق لا تستطيع دفع هذه المسؤولية إلا بإثبات السبب الأجنبي

(كالقوة القاهرة).

وهذا ما ذهب إليه جانب من الفقه(١)، من أن مسؤولية جهة التوثيق عن أي غلط أو قصور يرد في شهادة التوثيق هي مسؤولية مشددة (Open-ended liability).

وفي المقابل يلتزم البنك وعميله بمراعاة المصداقية والدقة في كافة البيانات التي يزود بها جهة التوثيق.

هذا ولم يرد في قانون التوقيع الإلكتروني المصري نص يلزم البنك وعميله بمراعاة الدقة والصدق في كافة البيانات التي تطلبها جهة التوثيق، وأن كان هذا لا يمنع من القول بالتزام البنك وعميله بهذا الأمر؛ باعتبار أن هذا الالتزام مما تفرضه قواعد العرف والعدالة وحسن النية في التعاقد، حتى ولو لم يرد النص عليه صراحة في العقد (المادة ١٤٨ مدني مصري).

هذا وقد نص القانون الأمريكي للاستخدامات العادلة للمعلومات (FIP Act)(٢) على هذا الالتزام صراحة، حيث نص على أن "على الشخص الملزم بإدلاء بيانات خاصة به لدى جهة تقدم له خدمة ما أن يراعى الدقة والأمانة في الإدلاء بها(٣).

٣- تلتزم جهة التوثيق بأن توضح للبنك وعميله الحالات التي يتم فيها

---

(١) **William Gram**; Op. Cit, p. ١٦.

(٢) هذا القانون متاح على العنوان الإلكتروني:
http://www.bobgellman.com/rg-docs/rg-fips.pdf

(٣) **David L. Baumer and others;** Op. Cit, p. ٤٠٣.

إيقاف العمل بشهادة التوثيق؛ وهي حالات ترتبط في الغالب بأنعام صلاحية الشهادة للاعتماد عليها في المعاملات.

٣٣٧- وتبدو أهمية تحديد هذه الحالات من قبل جهة التوثيق، بالنظر إلى اعتماد كل من البنك وعميله على هذه الشهادة في التعامل بينهما، ومن ثم إلغاء هذه الشهادة يعنى توقف هذا التعامل. أيضا يهم ذكر هذه الحالات لبيان الوقت الذي تبدأ فيه مسؤولية حامل الشهادة أو مسؤولية جهة التوثيق بحسب طبيعة السبب الذي يقف وراء الإلغاء ومدى قيام حامل الشهادة بإبلاغ جهة التوثيق بها من عدمه(١).

أيضا يجب على جهة التوثيق أن تحيط البنك وعميله علما بالإجراءات التي يجب أن تتبع في مثل هذه الحالات، مع بيان الوسيلة التي يتم بها الإبلاغ، والمواعيد التي يتم فيها.

وحسنا فعلت هيئة تنمية تكنولوجيا المعلومات المصرية، وذلك عندما فرضت في كراسة شروط الترخيص بتقديم خدمات التوقيع الإلكتروني، على جهة التوثيق تبنى نظام لإيقاف شهادة التصديق، كما عددت الحالات التي يجب فيها على الجهة إيقاف الشهادة، وهي(٢):

- العبث ببيانات الشهادة أو انتهاء مدة صلاحيتها

---

(١) د. **عبد الفتاح بيومي حجازي**، مرجع سابق، ص٢٠٧.

William Gram; Op. Cit, p. ١٦.

(٢) كراسة شروط الترخيص بتقديم خدمات التوقيع الإلكتروني، الأنظمة والقواعد، مادة ٣ فقرة (٦)، مرجع سابق، ص١٣.

- سرقة أو فقد المفتاح الشفري الخاص أو البطاقة الذكية، أو عند الشك في حدوث ذلك.

- عدم التزام الشخص المصدر له شهادة التصديق الإلكتروني ببنود العقد المبرم مع المرخص له.

هذا ولم يرد في كراسة الشروط ما يفيد إلزام جهة التوثيق بإعلام طالب الخدمة (البنك وعملائه) بالوسائل التي يمكن اتباعها للابلاغ الفوري عن وجود أحد الأسباب التي تدعو إلى إيقاف الشهادة.

وعن موقف التشريعات الأخرى التي نظمت حالات إيقاف شهادة التوثيق، فقد أولت اهتماما بتنظيم هذه الحالات، وذلك على التفصيل التالي:

أ- الإيقاف بناء على طلب البنك الإلكتروني أو عميله:

تلتزم جهة التوثيق الإلكتروني بإيقاف شهادة التوثيق متى طلب البنك الإلكتروني أو عميله ذلك. فشهادة التوثيق بالنسبة لمن صدرت لمصلحته حق شخصي، تحمل الصفات الشخصية له مثل اسمه وجنسيته وعنوانه وغيرها من البيانات الخاصة به، فهي أشبه ما تكون بالبطاقة الشخصية أو جواز السفر التي يستطيع بموجبها إجراء التعاملات في البيئة الافتراضية. لذلك يملك البنك الإلكتروني أو عميله في أي وقت التقدم بطلب لجهة التوثيق لإيقاف شهادة التوثيق لأسباب يقدرها البنك الإلكتروني أو عميله(١).

وقد نص القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية ٨٣ لسنة

---

(١) **William Gram**; Op. Cit, p. ١٦.

٢٠٠٠ في الفصل ٢٠ منه على أن "يوقف مزود خدمات المصادقة الإلكترونية حالا الشهادة عند طلب صاحب الشهادة".

وقد أعطى المشرع الإمارات في قانون إمارة دبي رقم (٢) لسنة ٢٠٠٢ بشأن المعاملات والتجارة الإلكترونية لصاحب شهادة التوثيق الحق في طلب إيقاف شهادة التوثيق حيث نص على التزام مزود خدمة التوثيق "أن يوفر وسيلة للموقعين تمكنهم من تقديم إشعار بأن أداة التوقيع قد تعرضت لما يثير الشبهة، وأن يضمن توفر خدمة إيقاف التوقيع في الوقت المناسب ".

والسؤال: هل يمكن لصاحب الشهادة سواء كان البنك الإلكتروني أو العميل أن يتقدم لجهة التوثيق بطلب لإلغاء الشهادة بعد أن اعتمد الطرف الآخر عليها في التعاقد؟

ذهب جانب من الفقه[١] إلى القول بأن جهة التوثيق يجب عليها أن تستجيب لطلب صاحب الشهادة في هذه الحالة، لأن عنصر الضرر واقع في دائرة العلاقة بين صاحب الشهادة والطرف الآخر معه في العلاقة، حيث يملك الأخير الرجوع على الأول في هذه الحالة بالتعويض، ومن ثم ليس هناك ما يدعو إلى رفض جهة التوثيق لهذا الطلب.

ويبدو لنا أن الأمر يحتاج منا إلى أن نفرق بين فرضين:

الأول: حسن نية مقدم الطلب، ويتحقق ذلك إذا كان مقدم الطلب لا يعلم بوجود الغلط في الشهادة، أو كانت قد سرقت منه، أو تم تعديل ما بها من بيانات دون أن يدري، هنا يجب أن تستجيب جهة التوثيق لمطلبه بإيقاف شهادة التوثيق.

---

(١) **د. عبد الفتاح بيومى حجازي**، مرجع سابق، ص١٨٢.

الثاني: سوء نية مقدم الطلب. ويتحقق ذلك إذا كان مقدم الطلب يهدف من ورائه إلى النكاية والتهرب من التزاماته تجاه الطرف الآخر، أو خديعته، هنا يجب أن ترفض جهة التوثيق مطلبه في إيقاف الشهادة؛ حيث تربو في هذه الحالة اعتبارات حماية الأوضاع الظاهرة وحسن النية في التعامل على اعتبارات كون الشهادة تمثل حقا شخصيا.

لذلك يجب على جهة التوثيق أن تنظر في الطلب المقدم إليها لإيقاف الشهادة وتقدر طبيعة الظروف والبواعث التي تقف وراء تقديمه.

أما عن الضرر الناجم عن اعتماد الطرف الآخر على بيانات الشهادة في التعاقد (كما لو لحق البنك ضرر نتيجة اعتماده على شهادة التوثيق التي تظهر سلامة مركز العميل المالي لمنحه قرض)، فهذه يكون الفيصل فيها الوقوف على السبب الذي أدى إلى تعيب الشهادة أو فقدها، سواء كانت جهة التوثيق أم صاحب الشهادة.

ب- وفاة العميل أو انقضاء الشخصية القانونية للبنك الإلكتروني:

من الحالات التي يمكن لجهة التوثيق أن تقوم على أثرها بإيقاف شهادة التوثيق هي انقضاء الشخصية القانونية لحامل الشهادة. فكما سبق أن ذكرنا شهادة التوثيق بالنظر إلى طبيعتها كوسيلة تعريف بالشخصية في البيئة الافتراضية حق شخصي لحاملها، ومن ثم لا مجال للحديث عن وجود الشهادة بعد انقضاء شخصيته القانونية سواء بالوفاة (العميل) أو بالحل (البنك الإلكتروني).

وقد نص على ذلك القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية ٨٣ لسنة ٢٠٠٠ في الفصل ٢٠ منه على " يلغي مزود خدمات المصادقة

الإلكترونية حالا الشهادة عند إعلامه بوفاة الشخص الطبيعي أو انحلال الشخص المعنوي صاحب الشهادة".

ج- وجود بيانات مغلوطة أو مزيفة أو وجود خلل في نظام عمل الشهادة:

تملك جهة التوثيق إذا ما تبين لها بعد إصدار الشهادة أن أحد البيانات فيها مغلوط أو غير مطابق للواقع، أو تم تعديله بالزيادة أو النقص فلها أن تقوم بإيقاف هذه الشهادة.

فقد يتضح لجهة التوثيق الإلكتروني بعد إصدار الشهادة أن بها بيانات مغلوطة أو مزيفة على الرغم من أنها صدرت صحيحة؛ وذلك كما لو قامت جهة التوثيق بإعطاء شهادة لشخص له ذات الاسم الثلاثي لصاحب الشهادة الأصلي، أو تبين لجهة التوثيق أن المعلومات التي أعطيت الشهادة على ضوئها غير صحيحة، أو حدث انتهاك لنظام عمل التوقيع الرقمي كان تم فك التشفير الخاص به، في مثل هذه الحالات يجب على جهة التوثيق أن تقوم بتعليق العمل بهذه الشهادة إلى أن تتأكد من صحة هذه الشهادة. فإذا أتضح لها عدم صحة الشهادة، أو وجود خلل في نظام عملها فأنها تقوم بإلغائها[١].

وقد نص القانون التونسي سالف الذكر في الفصل ١٩ منه على " يتولى مزود خدمات المصادقة الإلكترونية تعليق العمل بشهادة المصادقة حالا بطلب من صاحبها أو عندما يتبين:

- أن الشهادة سلمت بالاعتماد على معلومات مغلوطة أو مزيفة،

---

(١) د. **عبد الفتاح بيومي حجازي**، مرجع سابق، ص١٧٦ وما بعدها.

- أنه تم انتهاك منظومة إحداث الإمضاء،

- أن الشهادة استعملت بغرض التدليس،

- أن المعلومات المضمنة بالشهادة قد تغيرت".

وأيا ما كان السبب الذي يقف وراء إلغاء الشهادة يجب على جهة التوثيق أن تعلم صاحب الشهادة بهذا الإلغاء وسببه، وتقوم جهة التوثيق بنشر هذا القرار في السجل الإلكتروني الخاص بها وذلك حتى يتسنى لصاحب الشهادة، والغير الذي له مصلحة من المعارضة في هذا الإلغاء.

وقد عالج القانون التونسي سالف الذكر هذا الأمر في المادة ١٩ حيث نص على أن "يتولى مزود خدمات المصادقة الإلكترونية إعلام صاحب الشهادة حالا بالتعليق وسببه ويتم رفع هذا التعليق حالا إذا تبين صحة المعلومات المدونة بالشهادة واستعمالها بصفة شرعية، ويعارض صاحب الشهادة أو الغير في قرار مزود الخدمات الخاص بتعليق الشهادة من تاريخ نشره بالسجل الإلكتروني المنصوص عليه بالفصل ١٤ من هذا القانون".

ويقصد بمصطلح التعليق الذى استعمله المشرع التونسى وقف الشهادة بالمعنى المقرر فى القانون المصرى.

وبعد الانتهاء من عرض لأهم الالتزامات التي تقع على عاتق جهة التوثيق في مواجهة البنك وعملائه، نوضح أن الأصل في رسم حدود العلاقة التعاقدية بين جهة التوثيق والبنك هو حرية الطرفين في صياغة بنود العقد على النحو الذي يحقق مصالحهم. فليست هناك قوالب جامدة تنصب فيها علاقة جهة التوثيق بالبنك. وهذا ما أوضحه منتدى قانون وسياسية الإنترنت (ILPF)[1] الذي أوصى

الحكومات الوطنية بضرورة ترك مساحة واسعة من حرية التعاقد (Freedom of Contract) بين جهة التوثيق وعملائها، والاعتراف بالأثر القانوني الكامل (Give full legal effect) لاتفاقهم ما لم تكن هذه الاتفاقات مخالفة للنظام العام، بحيث تأتى التزامات الأطراف ملاءمة لطبيعة العلاقة بينهم في ضوء طبيعة المخاطر المرتقبة والوسائل الأمنية الكفيلة بمواجهة هذه المخاطر(١).

وحسنا ما أوصى به هذا المنتدى؛ فالتوثيق الإلكتروني يقوم على تقديم خدمات غاية في الأهمية بالنسبة للمعاملات الإلكترونية بصورة عامة والبنك الإلكتروني بصورة خاصة، وهي الخدمات الأمنية، الأمر الذي يجب معه كفالة حرية التعاقد كي تأتى هذه الخدمات مناسبة لطبيعة محل الحماية في ضوء المخاطر التي تهدده.

وقد أندفع القضاء الأمريكي متبنيا هذا الاتجاه ومقررا إضفاء القوة القانونية على كل ما جاء في تعاقدات جهة التوثيق مع عملائها حتى ولو كان الأمر يتعلق بشروط تعفى جهة التوثيق من المسؤولية (Exculpatory clauses). ففي أحد القضايا حكمت إحدى المحاكم الأمريكية بصحة الشروط الواردة في العقد الذي ينظم علاقة جهة التوثيق بعميلها، والتي تعفى هذه الجهة من المسؤولية عن سرقة البيانات الموجودة بأحد الأجهزة الملحقة بالموقع الإلكتروني بسبب سوء عمل أجهزة الإنذار الإلكتروني. وأيدت المحكمة موقفها هذا بحرية أطراف العلاقة في صياغة الشروط التي تحقق مصالحهم المشتركة، مادامت هذه الشروط لا تخالف

(١) **Working group on international consensus principles for electronic authentication**; Op. Cit, p. ٧.

النظام العام[١].

ويبدو لنا أن القضاء الأمريكي قد تخلا عنه التوفيق في فهم المقصود بترك مساحة واسعة من حرية التعاقد (Freedom of Contract) بين جهة التوثيق وعملائها، والذي يعنى كما جاء في تعليق منتدى قانون وسياسية الإنترنت (ILPF) على توصيته، بأن المقصود به أن تأتى خدمات التوثيق ملائمة لطبيعة محل الحماية في ضوء المخاطر التي تهدده. فالمخاطر التي تحيط بالتعاملات الإلكترونية متفاوتة ومتباينة؛ ومن ثم يكون مستوى التأمين مختلفا من حالة لأخرى، فمستوى التأمين لموقع يقدم خدمات معلوماتية لا يتناسب مع موقع لبنك يؤدى خدمات مصرفية عبر شبكة الإنترنت. ولهذا تكون هناك مساحة أوسع لملاءمة كل حالة ومتطلباتها الخاصة.

وبناءً على ما سبق يجب على البنك الإلكتروني أن يستفيد من ذلك في إلزام جهة التوثيق بتوفير أقصى درجات الحماية والتأمين، ولا يقبل بأية بنود تعفى هذه الجهة من مسؤوليتها عن تحمل تبعات نشاطها.

والسؤال: ماذا لو جاء العقد بين جهة التوثيق والبنك ينطوي على شروط تعفى هذه الجهة من المسؤولية؟

لا شك أن إدراج جهة التوثيق شروطا تعفيها من المسؤولية عن تبعات نشاطها، في ظل أهمية هذا النشاط وتأثيراه البالغ في تأمين البنك وتعاملاته على شبكة الإنترنت، يعد تعسفا من قبل جهة التوثيق في مواجهة البنك.

هذا وقد عالج المشرع المصري مثل هذه الحالة، حيث أعطى للمحكمة سلطة

---

(١) **William Gram**; Op. Cit, p. ١٨.

تعديل شروط العقد أو الإعفاء منها، حيث نصت المادة ١٤٩ من القانون المدني المصري على أنه " إذا تضمن العقد شروطا تعسفية جاز للقاضي أن يعدل هذه الشروط أو يقرر الإعفاء منها، وذلك وفقا ما تقضي به قواعد العدالة، ويقع باطلا كل اتفاق على خلاف ذلك".

أيضا نص القانون التجاري الموحد الأمريكي (UCC) على سلطة المحكمة في استبعاد أي بند أو شرط يرد في العقد تراه غير ملائم أو مناسب، أو حتى الحد من آثاره في العلاقة بين المتعاقدين(١).

ويضاف إلى هذا الموقف التشريعي، موقف فقهي يراعى الطبيعة الخاصة للمعاملات الإلكترونية، والتي يظهر فيها الفارق الواضح بين مقدم الخدمة (جهة التوثيق) ومن يحصل عليها (البنك وعملائه) من ناحية الإلمام بالجوانب الفنية والتقنية الخاصة بتأمين المعاملات على شبكة الإنترنت، الأمر الذي جعل هذا الفقه،(٢) يقرر إمكانية مطالبة البنك بإبطال العقد في هذه الحالة. وتبرير ذلك أنه على الرغم من أن المشرع قد أورد حالات إبطال العقد على سبيل الحصر وهي الغلط والتدليس والاستغلال والإكراه، إلا أن التطور الذي شهدته المعاملات

---

(١) (If the court as a matter of law finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract with out the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result).

Uniform Commercial Code, ١٩٩٧, (part٣) general obligation and construction of contract.

(٢) د. **خالد ممدوح إبراهيم**، حماية المستهلك في المعاملات الإلكترونية، مرجع سابق، ص٧٢.

القانونية بسبب هيمنة الوسائل الإلكترونية على مجريات هذه المعاملات أبقى على حالات البطلان سالفة الذكر، ولكنه فرض تبني مفاهيم مختلفة لها، تراعي حالة عدم المساواة بين طرفي التعاقد من ناحية المعرفة والخبرة التقنية، الأمر الذي يجعل الطرف الأكثر إلماما بالجوانب التقنية في مركز أقوى في مواجهة متلقي الخدمة، وذلك على النحو الذي يجعل الأخير عرضة للوقوع في الغلط أو التدليس نتيجة قلة خبرته، وليس نتيجة خديعته أو تضليله.

ونحن من جانبنا نؤيد هذا الفقه فيما ذهب إليه، خاصة إذا ما كان تعديل شروط العقد أو الإعفاء منها من شأنها أن تؤثر على مضمون العقد كله، لذلك يجب أن يمكن البنك من الحق في المطالبة بإبطال العقد في هذه الحالة. ويعد الإبطال للغلط من أقرب الحالات التي يمكن أن يلجأ لها البنك في مثل هذه الحالة[1]، وذلك لتزايد احتمالات وقوع البنك فيه؛ لقلة خبرته وعدم تبصره بالتفصيلات الفنية للخدمات الأمنية على شبكة الإنترنت.

وفي نهاية الحديث عن التزامات جهة التوثيق، نود الإشارة إلى أن ما سبق ذكره من التزامات تمثل الحد الأدنى لما يجب أن تظهر عليه علاقة جهة التوثيق بالبنك، بحيث يمكن إضافة التزامات أخرى تقتضيها طبيعة وحجم معاملات البنك وما يحتاج إليه ذلك من تأمين مناسب. يضاف إلى ذلك أن جهة التوثيق ليست

---

(١) ويقصد بالغلط كسبب من أسباب بطلان العقد " تصور ما يخالف الواقع؛ فهو وهم يقوم في ذهن المتعاقد فيتصور الأمر على خلاف حقيقته فيندفع للتعاقد" وللغلط أنواع عدة : (١) الغلط المانع من التعاقد. وهو الغلط الذي ينصب على طبيعة العقد، أو ذاتية المحل، أو في وجود السبب (٢) الغلط غير المؤثر. وهو كالغلط في الحساب أو غلطات القلم (٣) والغلط الذي يعيب الإرادة، ويشترط لإبطال العقد بسبب هذا الغلط أن يكون جوهريًا، وأن يتصل بالمتعاقد الآخر. انظر د. محسن عبد الحميد البيه، النظرية العامة للالتزامات (المصادر الإرادية)، مرجع سابق، ص ٣٢١ وما بعدها.

ملزمة في علاقتها بالبنك فقط بما نص عليه العقد من التزامات، ولكن أيضا بما يقتضيه طبيعة العقد في ضوء طبيعة محله وما تفرضه قواعد العدالة والعرف.

المبحث الثالث

المسئولية المدنية لجهة التوثيق في مواجهة البنك الإلكتروني

٣٣٨- بعد التعرض لتعريف أمن البنك على شبكة الإنترنت، وأهم صور الاعتداءات التي تنال منه، والتوثيق الإلكتروني وخدماته في نظام عمل البنك، وأهم الالتزامات القانونية الواقعة على عاتق جهة التوثيق في مواجهة البنك بمناسبة تقديم خدمات التوثيق، يحين الوقت للتعرض للمسئولية القانونية الناشئة عن الانتهاكات الأمنية، سواء على صعيد المعتدين على أمن البنك، بصور الاعتداءات المختلفة، أم على صعيد مسئولية جهة التوثيق باعتبارها الملتزمة

بتأمين تواجد البنك على شبكة الإنترنت، وتأمين معاملاته مع عملائه عبر هـــذه الشبكة.

لذلك يقسم هذا الفصل إلى مبحثين: المبحث الأول، لمعالجة صور المسئولية المترتبة على الانتهاكات الأمنية السابق ذكرها، والمبحـث الثـاني، للمـسئولية القانونية لجهة التوثيق في مواجهة البنك وعملائه، وذلك على التفصيل التالي:

٣٣٩- انطلاقا من أهمية التوثيق الإلكتروني في مجال عمل البنوك العاملة عبر شبكة الإنترنت عرضنا فيما سبق لتعريف التوثيق في مجال عمل هذه البنـــوك، ولصور الخدمات الأمنية التي يمكن أن تقدمها هذه الجهة للبنك الإلكتروني لتأمين موقعه الإلكتروني على الشبكة، وتأمين المعـاملات المـصرفية التـي يقـدمها لعملائه، وأهم الالتزامات التي تقع على عاتق جهة التوثيق في مواجهـة البنـك الإلكتروني. وحتى يكتمل البنيان فإنه يجدر بنا أن نختم لذلك ببيـان المـسئولية المدنية لجهة التوثيق في مواجهة البنك الإلكتروني، وذلك على النحو التالي:

المطلب الاول

المسئولية العقدية لجهة التوثيق في مواجهة البنك

٣٤٠- بعد التعرف على التزامات جهة التوثيق في مواجهة البنك، وقبل التعرض

للمسؤولية العقدية لهذه الجهة عن الإخلال بأحد هذه الالتزامات، تبدو أهمية الوقوف على طبيعة العقد الذي يحكم وينظم العلاقة فيما بينهما، وذلك لإبراز طبيعة مسؤولية جهة التوثيق عنها. لذلك سنعرض في البداية لتكييف العلاقة بين جهة التوثيق والبنك، ثم لأحكام المسؤولية العقدية على النحو التالي:

أ) التكييف القانوني لعلاقة جهة التوثيق بالبنك الإلكتروني:

٣٤١- يمكن القول، من خلال مطالعة النصوص القانونية المختلفة التي نظمت التزامات جهة التوثيق، أنها لم تتعرض من قريب أو بعيد لتحديد طبيعة هذا العقد، بل حتى الدراسات القانونية المتخصصة لم تتطرق لهذا هي الأخرى لهذا الأمر. ولعل هذا يجد تبريره لدينا في أمرين:

- حداثة هذا العقد وغلبة الطابع الفني على التزاماته، الأمر الذي دعا إلى تجنب إفراغه في قالب قانوني معين قد يفقده حرية التفاعل مع متطلبات أطرافه، ويحول دون التطور المنشود في خدمات جهة التوثيق.
- تعدد واختلاف طبيعة الالتزامات الملقاة على عاتق جهة التوثيق بموجب العقد الذي يحكم عملها، الأمر الذي يصعب من مهمة وضع تكييف قانوني منضبط لهذا العقد.

لهذه الأسباب يبدو لنا أن العقد الذي ينظم علاقة جهة التوثيق بالبنك هو من قبيل العقود غير المسماة، والتي تستمد أحكامها في الأساس مما اتفق عليه الأطراف، بالإضافة للقواعد العامة في العقود (التجارية والمدنية)، خاصة ما يتعلق منها بحسن النية وعدم التعسف في استخدام الحق.

ب) أحكام المسؤولية العقدية لجهة التوثيق:

٣٤٢- من المعلوم أن المسؤولية العقدية لا يثور الحديث عنها إلا عندما نكون بصدد عقد صحيح يحكم وينظم العلاقة بين أطرافه، ثم يقع إخلال بأحد الالتزامات التي نظمها هذا العقد. ولما كانت العلاقة بين جهة التوثيق والبنك يحكمها عقد ينظم هذه العلاقة فإن إخلال جهة التوثيق بأحد هذه الالتزامات (عدم التنفيذ الكلى أو الجزئي، أو المعيب، أو المتأخر للعقد) سيرتب مسؤوليتها العقدية عن هذا الإخلال(١).

وبناءً عليه فأي صورة من صور الإخلال تظهر في سلوك جهة التوثيق فيما يتعلق بتسليم الأجهزة والبرامج، أو بالمحافظة على سلامة المعلومات المتبادلة بين البنك الإلكتروني والعميل، أو ما يتعلق بسرية المعلومات، أو إصدار شهادة التوثيق لعملاء البنك الإلكتروني تؤدى إلى انعقاد المسئولية العقدية لجهة التوثيق في مواجهة البنك وعملائه(٢).

ويغلب أن يتمثل الإخلال من قبل جهة التوثيق في صورة التنفيذ المعيب للالتزامات، وذلك نظرا لطبيعة التزامات جهة التوثيق والتي يغلب عليها الطابع الفني(٣)، وذلك كما لو تم إفشاء سرية المعاملات المصرفية بين البنك الإلكتروني والعميل، بسبب يرجع إلى أن الأجهزة والبرامج التي قامت جهة التوثيق بتسليمها للبنك الإلكتروني بها أعطال فنية، أو أن تقنيات التشفير ليست قوية.

---

(١) **Rosa Julia-Barcel٥ -Thomas C. Vinje**, Electronic signatures, Computer Law & security Report Vol. ١٤ no. ٥ ١٩٩٨. p. ٣٠٩.

(٢) **Graham Smith**; Op. Cit, p. ٢٧٧.

(٣) د. محمد حسين منصور، مرجع سابق، ص ٨٥.

والسؤال: هل تنعقد المسئولية العقدية لجهة التوثيق لإخفاقها في تحقيق أيا من الالتزامات الواقعة عليها أم لعدم قيامها ببذل عناية معقولة لتنفيذ الالتزامات بغض النظر عن تحقق النتيجة؟ بمعنى آخر هل التزام جهة التوثيق هو التزام بتحقيق نتيجة أم ببذل عناية؟

يبدو لنا في ضوء طبيعة التزامات جهة التوثيق، وأهمية وخطورة فكرة الأمن في نظام عمل البنك أن جهة التوثيق ملتزمة بتحقيق نتيجة، وذلك للأسباب التالية:

الأول: طبيعة التزام جهة التوثيق، والذي يغلب عليه الطابع الفني في الأداء[١]، ومن ثم وجب أن يأتي التنفيذ مطابقا للمواصفات الفنية المتفق عليها.

الثاني: النتيجة في التزام جهة التوثيق يغلب عليها الطابع المؤكد وليس الاحتمالي[٢]؛ بمعنى أن بذل عناية معقولة من قبل جهة التوثيق يجعل حدوث النتيجة أمرًا مؤكدًا؛ فقيام هذه الجهة بتوفير الأجهزة والبرامج اللازمة واتخاذ إجراءات التأمين المناسبة أمر يغلب عليه الطابع المؤكد.

الثالث: الطبيعة الخاصة للمخاطر المحيطة بنظام عمل البنك على شبكة الإنترنت، والتي تقتضي تشديدا في مسؤولية جهة التوثيق، بما يتلاءم مع حجم وطبيعة هذه المخاطر.

وبناءً عليه نخلص إلى أن التزام جهة التوثيق هو التزام بتحقيق نتيجة، ومن ثم لا يحتاج البنك لإثبات مسؤوليتها إلى إثبات الخطأ، حيث أنه مفترض في

---

(١) د. **جمال عبد الرحمن محمد علي**، مرجع سابق، ص٩٤.
(٢) د. **محمد حسين منصور**، مرجع سابق، ص٨٦.

جانب جهة التوثيق، ولا يمكن لها دفع مسؤوليتها بإثبات أنها بذلت العناية اللازمة، بل يجب إثبات السبب الأجنبي؛ كإثبات خطأ البنك أو عميله في اتباع تعليمات الأمن.

ويجب أن نوضح أن تحقيق النتيجة كمعيار لتنفيذ المدين التزامه بصورة عامة ليس أمرا موحدا بصدد جميع الالتزامات، بل يختلف من التزام لآخر بحسب طبيعة كل التزام وبحسب طبيعة الظروف المحيطة به؛ فمثلا التزام مقاول البناء بإنشاء مبنى معين لا يتحقق إلا باستكمال هذا البناء على النحو المتفق عليه، أما التزام جهة التوثيق بتأمين معاملات البنك الإلكتروني فأنه يتحقق من خلال تنفيذ التزاماتها السابقة (تزويد البنك الإلكتروني بالأجهزة والبرامج اللازمة لتأمينه، والحفاظ على سرية وسلامة المعلومات الخاصة بتعاملات البنك الإلكتروني وعملائه، وإصدار شهادات التوثيق لعملاء البنك الإلكتروني) بالمعنى السابق حتى ولو لم يتحقق تأمين البنك. فطبيعة المعاملات الإلكترونية على شبكة الإنترنت تجعل من الصعب جدا القول بأن النتيجة المنتظرة من جهة التوثيق تأمين معاملات البنك بالمعنى الحرفي للعبارة، حيث تتدخل عوامل عدة بخلاف أنشطة جهة التوثيق لتحقيق هذه النتيجة، منها مثلا إهمال البنك أو عملائه في اتباع تعليمات الأمن، الأمر الذي يجعل مفهوم تحقيق النتيجة في نظام عمل جهة التوثيق هو تحقيق الالتزامات المتفق عليها مع البنك الإلكتروني والتي تنعكس على تحقيق أمن البنك على شبكة الإنترنت. وبناء عليه تتحقق النتيجة المرجوة من جهة التوثيق بوضع كافة الأجهزة والبرامج اللازمة لتأمين البنك ومعاملاته بالمواصفات المتفق عليها، وبإعلام البنك بكافة الإجراءات الأمنية الواجب اتباعها، بحيث إذا ما حدث انتهاك لأمن البنك خارج إطار كفاءة الأجهزة

والبرامج المقدمة واحتياطات الأمن الواجبة، فلا تنعقد مسؤولية جهة التوثيق عقديا عن ذلك.

والسؤال: ماذا لو لحق عميل البنك الإلكتروني ضرر من جراء إخلال جهة التوثيق بأحد التزاماتها التعاقدية مع البنك الإلكتروني؟

٣٤٣- سبق أن ذكرنا أن البنك الإلكتروني يتعهد في مواجهة العميل بتقديم خدمات التوثيق اللازمة له عن طريق جهة التوثيق التي يتعامل معها البنك، على نحو يجعل البنك الإلكتروني ملتزمًا في مواجهة العميل عن هذه الخدمات(١)، ومن ثم في حالة حدوث أي إخلال في حصول العميل على هذه الخدمات فأنه يملك الرجوع على البنك الإلكتروني بموجب قواعد المسؤولية العقدية لتعويض ما أصابه من ضرر(بذات القواعد التي يملك البنك الإلكتروني الرجوع بها على جهة التوثيق السابق ذكرها)، ويملك البنك الإلكتروني بعد ذلك الرجوع على جهة التوثيق بموجب العقد الذي يجمع بينهما.

وأخيرًا، هل يمكن أن تسأل جهة التوثيق في مواجهة البنك الإلكتروني وعملائه عن سلامة الأجهزة والبرامج؟

٣٤٤- كما سبق أن ذكرنا الالتزام بالسلامة يعد من الالتزامات العقدية، يفرض على المدين تنفيذ العقد دون أن يصيب الدائن بضرر، وعرفنا أن الفقه والقضاء يشترطان لإعمال الالتزام بالسلامة شرطين؛ الأول / أن ينطوي العقد على خطر يهدد أحد الطرفين؛ وذلك بتوافر مؤشرات خطرة في طبيعة التزامات المدين، والثاني/ أن يكون المدين بالالتزام محترفا، الأمر الذي يبرر تكليفه بمزيدا من

---

(١) انظر سابقا، ص ٦٥٠.

العناية والحرص في تنفيذ العقد، ومن ثم لا يسأل عن هذا الالتزام إلا من كان يتمتع بخبرة عالية تمكنه من بذل من العناية والحرص ما لا يقدمه الشخص العادي[1].

وبتطبيق ذلك على جهة التوثيق، نجد أنها تحترف تقديم الخدمات الأمنية في المعاملات الإلكترونية؛ حيث إنها تباشر هذا العمل بصورة مطردة بغرض تحقيق الربح، كما أن نشاط هذه الجهة ينطوي على مخاطر جمة قد تصيب البنك الإلكتروني، فلاشك في اعتماد البنك على هذه الجهات في تأمين وجوده ونشاطه على شبكة الإنترنت، وذلك من خلال مجموعة من الأجهزة والبرامج قد يؤدى استعمالها إلى مخاطر تعصف بنشاط البنك بالكلية، خاصة في ظل شبكة عالمية مفتوحة على العالم كشبكة الإنترنت، الأمر الذي يؤكد ضرورة التزام جهة التوثيق بسلامة هذه الأجهزة والبرامج في مواجهة البنك، سواء ورد نص صريح بذلك في العقد الذي ينظم العلاقة بينهما أم لا.

ولاشك أن مثل هذا الالتزام يعد ضمانة كبيرة للبنك في مواجهة جهة التوثيق، حيث أنه يفرض مسؤولية مشددة على عاتق هذه الجهة مما يجعلها مسئولة عن كل الأضرار التي تلحق بالبنك من جراء المخاطر الناجمة عن عمل هذه الأجهزة دون أن يكلف البنك بإثبات خطأ جهة التوثيق، حيث إن خطأها مفترض. يضاف إلى ذلك أن جهة التوثيق لا تستطيع أن تدفع مسؤوليتها إلا بإثبات السبب الأجنبي.

لكن يجب ملاحظ أن مسؤولية جهة التوثيق عن سلامة الأجهزة والبرامج

---

(١) انظر سابقا، ص ٨٣.

ليست مسؤولية مطلقة، بل هي مقيدة بضرورة مراعاة البنك لأصول وقواعد الاستخدام السليم في ضوء تعليمات وإرشادات جهة التوثيق، وذلك على النحو الذي تنتفي فيه مسؤولية جهة التوثيق إذا استطاعت أن تثبت خطأ البنك في استعمال الأجهزة على النحو الذي الحق به الضرر، حيث تنتفي في هذه الحالة علاقة السببية بين نشاط جهة التوثيق والضرر الذي أصاب البنك.

المطلب الثانى

المسؤولية التقصيرية لجهة التوثيق الإلكتروني

٣٤٥- تقوم المسؤولية التقصيرية على أساس فكرة الخطأ أو العمل غير المشروع الناتج عن التزام غير عقدي يقضى بالتزام الكافة ببذل العناية اللازمة في السلوك وعدم الإضرار بالغير.

هذا ولا يوجد في النظام القانوني المصري نص خاص يفرض على جهة التوثيق التزاما بتأمين معاملات البنك على شبكة الإنترنت. ولا يوجد في هذا القانون سوى نص المادة ١٦٣ مدني مصرى والتي تقضى بمسؤولية كل مخطئ يتسبب في إلحاق الضرر بالغير، وذلك بمقتضى التزام عام مفروض على الكافة بعدم الإضرار بالغير[١].

على صعيد آخر، اهتم القانون الأمريكي بمعالجة التزام جهة التوثيق بتأمين معاملات البنك بنص خاص؛ حيث جعل هذه الجهة مسئولة عن كافة المخاطر

(١) تنص **المادة ١٦٣ من القانون المدني المصري** على أن "كل خطأ سبب ضررا للغير يلزم من ارتكبه بالتعويض".

التي تلحق البنك وعملائه نتيجة خطأ وإهمال جهة التوثيق في اتخاذ الاحتياطات الكفيلة بمواجهة هذه المخاطر[1].

وعلى الرغم من أن اتخاذ الاحتياطات الكفيلة بمواجهة كافة أنواع المخاطر هي من أهم الالتزامات العقدية التي تقع على عاتق جهة التوثيق، والتي يترتب على مخالفاتها المسؤولية العقدية، إلا أن موقف القانون الأمريكي من جعله التزاما قانونيًا يترتب على مخالفته المسئولية التقصيرية يجد تبريره لدينا في معالجة أي ضرر ناجم عن إهمال جهة التوثيق في تأمين معاملات البنك وعملائه، حتى لو كان هذا الإهمال لا يشكل خطأ عقديًا؛ وذلك كما في الحالات التي تفشى فيها جهة التوثيق سرية البيانات التي تطلع عليها قبل التعاقد مع البنك، ثم تسفر المفاوضات عن عدم إتمام العقد، أو يتم العقد ثم يقضى ببطلانه فيما بعد.

يضاف إلى أهمية وجود نص يعالج التزام جهة التوثيق، محاولة إعطاء الفرصة لعملاء البنك في حالة إصابتهم بضرر بالرجوع علي جهة التوثيق، التي لا يوجد عقد ينظم العلاقة بينهما.

والسؤال ما هو المعيار الذي على أساسه يقاس خطأ جهة التوثيق في علاقتها بالبنك وعملائه؟

ذهب جانب من الفقه[2] إلى القول بأن معيار خطأ جهة التوثيق في هذا النوع من المسؤولية يقاس بمعيار موضوعي، يقدر بالنظر إلى السلوك المعتاد

---

(١) **David L. Baumer and others;** Op. Cit, p. ٤٠٩.

(٢) **William Gram**; Op. Cit, p١٨.

في أعمال التوثيق الإلكتروني على شبكة الإنترنت وما يحتاج إليه ذلك من عناية ويقظة وتبصر من قبل جهة التوثيق. ولما كانت أنشطة التوثيق الإلكتروني من الحداثة بمكان على النحو الذي يصعب معه القول بوجود سلوك معتاد من العناية تلتزم به جهات التوثيق، فأن هذا الفقه أستطرد قائلا: أن المعيار المعتاد لجهة التوثيق هنا يقاس بالمعيار السائد في العناية للالتزامات الإلكترونية، وذلك في ضوء مجموعة من المؤشرات:

- مقدار الضرر المتوقع.
- صعوبة الخدمات الأمنية على شبكة الإنترنت.
- علاقة الأطراف المتعاقدة.

ونحن من جانبنا نتفق مع هذا الرأي على ضرورة تبنى معيار موضوعي لقياس خطأ جهة التوثيق، حيث أنه يفرض على الملتزم أن يأتي بمقدار من العناية محدد يتناسب مع الطبيعة الخاصة لأمن البنك على شبكة الإنترنت في ضوء الأهمية الكبرى للأمن في نظام عمل البنك، والمخاطر المحيطة به. لكننا نضيف إلى ذلك إلى أن يؤخذ في الاعتبار عند تقدير عناية جهة التوثيق في ضوء المعايير الموضوعية السابقة أمران:

- الطبيعة الخاصة لأمن البنك؛ هذه الخصوصية تتأبى على الخضوع للمعيار السائد في العناية في الالتزامات الإلكترونية بصورة عامة.

- أن جهة التوثيق تحترف تقديم الخدمات الأمنية، الأمر الذي يفرض عليها ضرورة تحمل مزيد من الاهتمام والعناية وفقا لمعيار الشخص الحريص، وليس السلوك المعتاد.

وبناء عليه يقاس الخطأ التقصيرى لجهة التوثيق بمعيار موضوعي يراعى احتراف هذه الجهة تقديم الخدمات الأمنية، والطبيعة الخاصة للمخاطر المحيطة بالبنك على شبكة الإنترنت، الأمر الذي يتطلب معاملة أمنية خاصة، بما سيجعل مسؤولية جهة التوثيق عن أخطائها في مواجهة البنك أو أي من عملائه مسؤولية مشددة.

نخلص من كل ذلك إلى أن جهة التوثيق مسؤولة في مواجهة البنك وعملائه عن أخطائها الشخصية خارج نطاق العقد الذي ينظم العلاقة بينهم(١) والأمر الذي سيزيد من فرص الضمان للبنك وعملائه، وذلك لتغطية كل حالات الخطأ التي تصدر عن جهة التوثيق في مواجهة البنك وعملائه، حتى ولو لم تشكل انتهاكا لأحد الالتزامات العقدية.

المطلب الثالث

مسؤولية جهة التوثيق عن أخطاء العاملين لديها:

٣٤٦- تسأل جهة التوثيق مدنيا في مواجهة البنك وعملائه عن أخطاء العاملين لديها بموجب نص المادة ١٧٤ من القانون المدني المصري، والتي تنص على أن "يكون المتبوع مسئولا عن الضرر الذي يحدثه تابعه بعمله غير المشروع متى كان واقعا منه حالة تأدية وظيفته أو بسببها".

فقد وضع هذا النص أساسا لمسئولية جهة التوثيق عن أعمال العاملين لديها، مادامت هناك علاقة تبعية بينها تملك جهة التوثيق بموجبها سلطة إصدار الأوامر

---

(١) **William Gram**; Op. Cit, p١٨

والتوجيهات لهؤلاء العاملين، سواء كانت هذه السلطة مستمدة من العقد (كعقد العمل) أو غير مستمدة منه، وأن يقع الخطأ من هذا العامل أثناء وظيفته أو بسببها.

ولاشك أن مثل هذه المسئولية من شأنها أن تزيد من ضمانات البنك في مواجهة جهة التوثيق، حيث يملك البنك الرجوع ليس فقط على جهة التوثيق، ولكن على العاملين لديها مباشرة، أو عليهما معا وفقا لما يحقق له مصلحة أكبر. هذا من ناحية، من ناحية أخرى لا تملك جهة التوثيق في حالة تحقق شروط المسئولية أن تدفعها بإثبات انتفاء الخطأ من جانبها، أو انعدام علاقة السببية بين خطئها والضرر الذي وقع، حيث تأسس هذه المسؤولية على أساس فكرة الخطأ المفترض، ومن ثم تعتبر مسؤولية مشددة لجهة التوثيق. لكن هذا لا يمنع جهة التوثيق من إمكانية دفع هذه المسؤولية من خلال إثبات انتفاء خطأ العامل، وعدم وجود علاقة سببية[1]

المطلب الرابع

مسؤولية جهة التوثيق باعتبارها حارسا للأشياء

٣٤٧- نص القانون المدني المصري في المادة ١٧٨ منه على أن " كل من تولى حراسة أشياء تتطلب حراستها عناية خاصة أو حراسة آلات ميكانيكية يكون مسئولا عما تحدثه هذه الأشياء من ضرر، ما لم يثبت أن وقوع الضرر كان بسبب أجنبي لا يد له فيه".

---

(١) د. محسن عبد الحميد البيه، مرجع سابق، ص ١٨٣؛ أيضا د. أحمد شوقي عبد الرحمن، مرجع سابق، ص٣٢٧.

وقد ضع هذا النص شرطين لقيام مسئولية حارس الأشياء عن الضرر الصادر عن الأشياء التي في حراسته: الأول وجود حراسة على الشيء، الثاني تدخل إيجابي من هذا الشيء لإحداث الضرر، حيث لا يكفى التدخل السلبي، ويجب على المضرور إثبات هذا التدخل(١).

وكما سبق أن ذكرنا (٢) أن الفقه والقضاء في مصر قد استقرا على تحديد مفهوم الحراسة في ضوء نص المادة ١٧٨ من القانون أخذا بنظرية الحراسة الفعلية؛ تلك التي تقضى بأن الحارس هو ذلك الشخص الذي يتمتع بسلطات الاستعمال والتوجيه والرقابة على الشيء لحساب نفسه بصورة مستقلة، وذلك بصرف النظر عن وجود سند قانوني يبرر حيازة الحارس للأشياء التي في حيازته.

أيضا تعرفنا على أن الكمبيوتر والبرامج الملحقة به تعد من قبيل الأشياء التي تحتاج إلى عناية خاصة وفقا لنص المادة ١٧٨، وذلك بالنظر إلى طبيعتها وطبيعة البيئة التي تعمل فيها.

وبإنزال ذلك على جهة التوثيق، يمكن القول بانعقاد مسؤوليتها بوصفها حارسا للأشياء عما تسببه الأجهزة والبرامج التي زودت البنك بها من ضرر، مادامت قد تحققت لها الحراسة الفعلية على هذه الأشياء؛ بمعنى وجود سلطة فعلية لجهة التوثيق تمتلك بموجبها ممارسة سلطات الرقابة والاستعمال والتوجيه على هذه الأجهزة والبرامج، سواء كانت هذه الأجهزة في حيازتها أم كانت في حيازة البنك، مادامت جهة التوثيق تحتفظ لنفسها بهذه السلطات بصورة مستقلة.

---

(١) د. **أحمد شوقي عبد الرحمن**، المرجع السابق، ص٣٢٩.

(٢) انظر سابقا، ص ٩٥.

ولا يكلف البنك إقامة مسؤولية جهة التوثيق بوصفها حارسا للأشياء إثبات خطئها، حيث إن الخطأ مفترض في جانبها، ولا يكفي جهة التوثيق لدفع مسؤوليتها في هذه الحالة إثبات انتفاء الخطأ، ولا يمكنها التخلص من المسؤولية في هذه الحالة إلا بإثبات السبب الأجنبي؛ كقوة قاهرة أو حادث فجائي.

أما إذا كان تسليم جهة التوثيق هذه الأشياء للبنك الإلكتروني على نحو يجعل البنك هو صاحب السلطة الفعلية على هذه الأشياء، فإن الحراسة في هذه الحالة تنتقل من جهة التوثيق للبنك، ومن ثم يكون الأخير هو المسئول عن ما تسببه هذه الأجهزة من ضرر.

٣٤٨- والسؤال: هل يعتبر العامل لدى جهة التوثيق حارسا للأجهزة والبرامج التي يستعملها لأداء مهام عمله لدى جهة التوثيق، ومن ثم يمكن أن يسأل عن الضرر الناتج عن عمل هذه الأجهزة في مواجهة البنك، وعملائه؟

اختلف الفقه في سبيل الإجابة على هذا التساؤل إلى رأيين:

الأول: أن العامل لدى جهة التوثيق يسأل بوصفه حارسا عما تسببه الأجهزة التي توجد تحت حيازته إذا ما كان يستعمل هذه الأجهزة لتحقيق منفعة خاصة به[1].

الثاني: أن العامل لدى جهة التوثيق لا يكون مسئولا عما تحدثه هذه الأجهزة من ضرر بوصفه حارسا، وذلك حتى لو تركت له جهة التوثيق حرية استعمال الشيء، مادامت تقصد من وراء هذا الاستعمال تحقيق مصلحتها (جهة

---

(١) انظر هذا الرأي لدى د. **محمد لبيب شنب**، المسئولية عن الأشياء، مرجع سابق، ص ١٢٧، ١٢٨.

التوثيق)[1].

ونحن من جانبنا نقر بصحة الرأيين السابقين فيما ذهبا إليه، ولا نرى تعارضا بينهما في ذلك. فقد استقر كل منهما على مبدأ واحد وهو أن الحراسة لا توجد مع وجود علاقة التبعية. فطبقا للرأي الأول العامل لدى جهة التوثيق مسئول بوصفه حارسا إذا استجمع مقومات الحراسة، المادية (استعمال، توجيه، رقابة)، والمعنوية (إذا كان يمارس هذه السلطات لحساب نفسه وليس لحساب جهة التوثيق) وهو في هذه الحالة لا يعد تابعا لجهة التوثيق فيما يقوم به من عمل، وطبقا للرأي الثاني العامل لدى جهة التوثيق لا يسأل عن الأضرار التي تسببها الأجهزة إذا كان يملك سلطات الاستعمال والتوجيه عليها، ولكنه يمارسها لمصلحة جهة التوثيق، أي تتحقق التبعية في جانبه، ومن ثم لا يعد حارسا.

وبناءً عليه، لا يسأل العامل لدى جهة التوثيق في مواجهة البنك بوصفه حارسا متى كان استعماله لهذه الأجهزة لحساب ومصلحة جهة التوثيق.

٣٤٩- وأخيرا، وفي ظل الأهمية التي تضطلع إليها جهة التوثيق الإلكتروني في نظام عمل البنك وتشغيله، من خلال تولى مهمة تأمين البنك ومعاملاته على شبكة الإنترنت يثور تساؤل حول مدى كفاية قواعد المسؤولية العقدية والتقصيرية لمواجهة كافة أشكال المخاطر المختلفة التي يمكن أن تلحق بالبنك الإلكتروني وعملائه؟

ذهب جانب من الفقه[2] في سبيل الإجابة على هذا التساؤل إلى القول بأن

(١) د. **أحمد شوقي عبد الرحمن**، مرجع سابق، ص ٣٤٦.
(٢) **William Gram**; Op. Cit, p. ١٩.

جهة التوثيق تكون مسئولة عن الأضرار التي تلحق البنك وعملاءه بسبب المخاطر الناجمة عن نشاطها. وقد اعتمد هذا الفقه في سبيل تبرير رأيه على القول بأن القاضي، وهو ينظر النزاع، يستطيع أن يفسر العقد على النحو الذي يجعل جهة التوثيق مسئولة عن مثل هذه المخاطر.

وعلى الرغم من وجاهة هذا الرأي فيما توصل إليه من ضرورة تحمل جهة التوثيق المسؤولية عن مثل هذه المخاطر، إلا أن التبرير الذي قام عليه هذا الرأي يبدو أنه قد بالغ في فهم المقصود بسلطة القاضي في تفسير العقد الذي يحكم العلاقة محل النزاع. فإذا كان من صميم عمل القاضي تفسير بنود العقد في ضوء حرفية نصوصه، بل ومحاولة تفسير الإرادة الضمنية للأطراف في ضوء قواعد العرف والعدالة، إلا أن ذلك لا يعنى إضافة أمور غير موجودة أصلا بالعقد، حتى لا يعد ذلك اعتداءً على مبدأ سلطان الإرادة.

والقول عندنا في هذا الصدد أن السياسة التشريعية في النظم القانونية المختلفة أصبحت لا تعتمد بالكلية على فكرة الخطأ كأساس للمسئولية، حيث إن هذا الأساس قد شهد تطورا في مفهومه بسبب الاعتماد على وسائل التقنية الحديثة في تنفيذ الالتزامات القانونية. وقد كان من أهم صور التطور في هذا المجال قواعد المسؤولية الموضوعية (تحمل التبعة)، تلك القواعد التي تقضى بمسؤولية كل شخص ينطوي نشاطه على مخاطر، وذلك إذا ما نتج عن هذا النشاط ضرر أصاب الغير، يستوي أن يجمعه بهذا الغير رابطة عقدية أم لا، ويستوي أن يثبت الخطأ في جانب هذا الشخص أم لا، حيث يكتفي هذا النوع من المسؤولية بركنين فقط هما الضرر وعلاقة السببية.

وبناءً عليه تكون جهة التوثيق مسئولة عن الأضرار التي تلحق البنك

الإلكتروني وعملائه بسبب نشاطها في تأمين وجود البنك الإلكتروني وعمله على شبكة الإنترنت، حتى ولو كان نشاط جهة التوثيق لم يصل إلى حد الخطأ سواء في مفهوم المسؤولية العقدية أم التقصيرية. فجهة التوثيق ذات أهمية كبرى في نظام عمل البنك الإلكتروني، هذه الأهمية تنبثق عن دورها المحوري في تأمين وجود البنك وتعاملاته من خلال توفير الأجهزة والبرامج الأمنية، الأمر الذي يجعل نشاطها محفوفا بالمخاطر، ويجعل إثبات الخطأ والتقصير في جانبها أمرا صعبا، لذلك تقتضي أبسط قواعد العدل والمنطق مسؤولية جهة التوثيق عن الأضرار الناجمة عن نشاطها في تأمين البنك وعملائه[1]؛ حيث يكفي البنك أو عميله في حالة أن أصابهم ضرر نتيجة نشاط جهة التوثيق الرجوع عليها مباشرة دون أن يكونوا مكلفين بإثبات الخطأ في جانبها، ولا تستطيع جهة التوثيق في هذه

---

(١) د. **شريف محمد غنام**، مسؤولية البنك عن أخطأ الكمبيوتر في النقل الإلكتروني للنقود، مرجع السابق، ص ١٠٥؛ د. **نورى حمد خاطر**، المرجع السابق، ص١٨٣٣؛ د. **حسن عبد الرحمن قدوس**، المرجع السابق، ص ٥٦.

وقد جاء في **الوثيقة الاستشارية الصادرة عن وزارة الصناعة البريطانية** مستوى المسئولية التي يجب أن تتطلع إليها جهة التوثيق الإلكتروني في مواجهة عملائها.

(The level of liability it would be appropriate to expect such trust service providers to undertake. It is essential that such limits be sufficient to provide the consumers of the services they offer some measure of confidence that their potential losses would be compensated in the event that something went wrong. However, it is equally clear that the attractions of becoming a trust service provider would be limited if the law required them to take on unlimited liability for the potential losses of their customers and those who relied upon any certificates which they might produce.)

Kit Burden: Op. Cit. p. ٢٥٠.

الحالة أن تدفع مسؤوليتها إلا بإثبات السبب الأجنبي كالقوة القاهرة[١].

٣٥٠- وأخيرا يجدر بنا الإشارة إلى أن جهة التوثيق الإلكتروني ليست مكلفة بتحقيق الأمن المثالي والتام (perfect security)[٢] في علاقتها بالبنك وعملائه؛ حيث إن هذا أمر مستحيل التحقق، ولكنها مكلفة بتحقيق أقصى درجات الحماية في نطاق المألوف في مثل هذه المعاملات، بما يتناسب مع خصوصية النشاط المصرفي الإلكتروني على شبكة الإنترنت، بحيث يمكن القول؛ بانعقاد المسؤولية العقدية لجهة التوثيق إذا ما خالفت أحد الالتزامات الواردة في العقد الذي يحكم علاقتها بالبنك. كما تنعقد مسؤوليتها التقصيرية عن أي خطأ يسبب ضررا للبنك أو عملائه خارج نطاق الالتزامات العقدية، أيضا تسأل جهة التوثيق عن كل ضرر ناتج عن نشاطها حتى ولو لم يصل هذا النشاط إلى حد الخطأ. أما ما يحدث من ضرر يصيب البنك أو عملائه خارج هذا النطاق فلا تسأل عنه جهة التوثيق؛ فلو كان مصدر الضرر سبب أجنبي كقوة قاهرة أو حادث فجائي أو خطأ البنك في مراعاة تعليمات الأمن فهنا لا تكون جهة التوثيق مسئولة. فلا يمكن القول بإطلاق العنان لمسؤولية جهة التوثيق عن كافة الأضرار التي تلحق بالبنك أو عملائه، حيث إن مثل هذا القول يعد إجحافا شديد بهذه الجهة، ومغالاة في مسؤوليتها على النحو الذي يتنافى مع قواعد العدالة والمنطق، ودعوة إلى إبعاد هذه الجهات عن العمل في مجال تأمين المعاملات المصرفية على شبكة الإنترنت بما سيكون له سيء الأثر على مستقبل هذه البنوك.

---

(١) د. محمد حسين منصور، مرجع سابق، ص ٤٠١

(٢) **Graham Smith**; Op. Cit, p. ٢٧٩.

الخاتمة

عكست هذه الدراسة خلال مراحلها المختلفة الأهمية القصوى التي يضطلع بها البنك الإلكتروني على شبكة الإنترنت، ككيان اقتصادي أضحى المحدد الاستراتيجي لوجود وفعالية التجارة الإلكترونية على شبكة الإنترنت، وذلك من خلال هيمنته على نظم الدفع الإلكتروني الخاصة بهذه التجارة، ومن خلال تقديم غيرها من العمليات المصرفية الإلكترونية التي تتناسب مع متطلبات هذه التجارة، وتلبى رغبات المتعاملين (خاصة التجار)؛ من خلال الابتعاد عن الروتين البنكي الذي تشهده البنوك التقليدية، والذي لا يتناسب البتة مع إيقاع الحياة التجارية، الذي يزداد يوما تلو الآخر سرعة في الأداء.

وإيمانا بأن التنظيم القانوني الجيد هو خير مرشد وممهد لهذا الوافد الجديد في بيئة شديدة الوعورة، وإيمانا بأن هذا التنظيم لن يؤتى ثماره المرجوة إلا بإدراك قوى وبصيرة واعية لواقع هذا البنك، ومقدرا للاعتبارات المختلفة التي تؤثر وتتحكم في وجوده وتشغيله، فقد كانت هذه الدراسة، التي سعت لتحقيق أهدافها تلك، من خلال إيجاد تغطية شاملة لكافة القضايا القانونية ذات الصلة بعمل هذا البنك.

وقد اقتضى التنظيم القانوني لهذا البنك عرضًا سريعًا للتكوين الفني للبنك، بهدف تقريب الرؤية قدر الإمكان حول الكيفية التي يتم تشغيل البنك بها، وذلك حتى يأتي تأسيس وتأصيل العلاقات القانونية التي تجمع البنك بمقدمي هذه الخدمات من ناحية، وبعملائه من ناحية أخرى في ضوء فهم حقيقي وواقعي لطبيعة عمل هذا البنك. وذلك من باب أن التأصيل القانوني يبدأ بالفهم الجيد

لواقع الأمر.

كما تبين من خلال هذه الدراسة أيضا أهمية الدور الذي يلعبه مقدمو الخدمات الإلكترونية في نظام عمل هذا البنك، هذا الدور الذي فرضته الطبيعة الإلكترونية لشبكة الإنترنت، والذى يحتاج إلى ذوى الخبرة في هذا المجال ليأخذوا بيد البنك، الأمر الذي اقتضى إيجاد تنظيم قانوني مفصل للعلاقات التي تجمع البنك بهؤلاء، والمسئوليات الناشئة عن هذا، وذلك في ضوء الطبيعة الخاصة للعمل المصرفي، والتي تفرض بعض الالتزامات التي لا تعرفها سائر المعاملات التجارية الأخرى، أو لا تعرفها بذات الأهمية، وذلك كسرية وأمن المعاملات المصرفية، والتي يرتبط وجود البنك بها. فقد ألقت هذه الاعتبارات بظلالها على التزامات مقدمي الخدمات الإلكترونية في مواجهة البنك، من خلال تبنى مفاهيم قانونية مشددة لهذه الالتزامات والمسؤوليات المترتبة على الإخلال بها، وذلك كي تلبى المتطلبات الخاصة للبنك وطبيعة عمله، ومن ثم تأتى بالنتائج المرجوة من نظام عمل البنك على شبكة الإنترنت. أيضا ظهرت في نظام عمل البنك التزامات جديدة لم يكن يعرفها العمل المصرفي من قبل، تمثلت في تقيده بالاعتبارات المختلفة للملكية الفكرية، والتي فرضتها عليه حاجته في الحصول على البرامج المعلوماتية بأنواعها المختلفة ممن لهم عليها حق ملكية فكرية، بل أظهرت الدراسة أن حاجة البنك لهذه البرامج لا تتوقف عند حد استعمالها، بل قد تمتد إلى الرغبة في إعادة نسخها للعملاء لاعتبارات يقدرها البنك وتقتضيها طبيعة المعاملات المصرفية، الأمر الذي يدفع بالبنك للحصول على ترخيص بإعادة نسخها. أيضا يلتزم البنك بالمحافظة على ما يتم تصميمه على موقعه من أشكال وتصميمات تحمى بموجب قوانين حماية الملكية الفكرية.

وأظهرت هذه الدراسة كذلك الدور البالغ الأهمية للرقابة على إنشاء وتشغيل البنك الإلكتروني على شبكة الإنترنت. هذه الرقابة التي ظهرت بثوب جديد، فرضه حجم ونوعية المخاطر التي تحيط بهذا البنك، والتي ظهرت في صورة تحديات حقيقية يتوقف عمل هذا البنك من عدمه على التعامل معها. فقد سلطت هذه الدراسة الضوء على أهم أنواع المخاطر التي استجدت مع ممارسة البنك لنشاطه على شبكة الإنترنت، كما أظهرت كيف أن هذه المخاطر تضرب بعمق في وجود البنك، وكيف أنها استدعت تحصنه بمجموعة من مقومات الوقاية تحت سمع وبصر جهة الرقابة، والتي تعمل على التأكد من توافر هذه المقومات قبل أن تمنحه الترخيص بممارسة العمل المصرفي على شبكة الإنترنت.

هذا بالإضافة إلى ممارسة رقابة دورية بعد الإنشاء، تهدف إلى التأكد من استمرار توافر هذه المقومات بما يتناسب مع نوعية وحجم المخاطر المستجدة. أيضا أظهرت هذه الدراسة بعدا جديدا في نظام عمل البنك الإلكتروني على شبكة الإنترنت يتطلب استعدادات خاصة من قبل جهة الرقابة؛ وهو البعد الدولي لنشاط هذا البنك، وذلك على النحو الذي تظهر معه الحاجة ماسة لوجود تعاون دولي فيما بين جهات الرقابة الوطنية، من أجل التوصل لصيغة قانونية موحدة، يمكن معها تفادى وجود تصادم بين النظم القانونية المختلفة.

كما أولت هذه الدراسة اهتماما كبيرا بالأبعاد القانونية الجديدة في علاقة البنك الإلكتروني بعملائه، وذلك من خلال إبراز أهم القضايا القانونية التي تثيرها علاقة البنك بعميله في هذا العالم الافتراضي. وقد عرضت هذه الدراسة لذلك من خلال تناول للتنظيم القانوني الذي يسرى على كافة التعاقدات المصرفية؛ والذي خطى أولى خطواته بالوقوف على مفهوم واضح للعقود المصرفية على شبكة

الإنترنت، وأهم ما تتمتع به من خصائص ذات بعد قانوني، ثم تلا ذلك التعرض للقواعد التي تحكم إعلان البنك عن خدماته المصرفية، مرورا بتعاقد العميل مع البنك بشأن هذه الخدمات- مع التعرض لأوجه الخصوصيات القانونية للتعاقد المصرفي، وكيف احتفظ بها البنك في تعامله عبر شبكة الإنترنت- وانتهاءً بحصول العميل على هذه الخدمة.

أيضا، سلطت هذه الدراسة الضوء على أهم نماذج العمليات المصرفية للبنك على شبكة الإنترنت، وهى إصدار النقود الإلكترونية، والتحويل الإلكتروني للنقود، والتعرض لأهم خصوصيات هذه العمليات، وما أثاره تقديم البنك لها عبر شبكة الإنترنت من قضايا.

كما أبت هذه الدراسة أن تستكمل بنيانها إلا بعد عرض مفصل للتنظيم القانوني لأمن البنك الإلكتروني على شبكة الإنترنت، والذي يلعب دورا بالغ التأثير في نظام عمل هذا البنك، الأمر الذي اقتضى التعرض لمفهوم أمن هذا البنك، وإظهار أوجه الاختلاف بينه وبين أمن البنك التقليدي، والذي عكسته طبيعة محل الحماية، واختلاف المناخ الذي يمارس فيه العمل المصرفي.

وأظهرت هذه الدراسة كذلك، صور الاعتداءات التي تستهدف أمن هذا البنك، والتعرض للمسؤولية الجنائية والمدنية للمعتدى، ومدى مسؤولية البنك والعاملين لديه في مواجهة العميل. أيضا تعرضت هذه الدراسة للتنظيم القانوني لعلاقة البنك بجهة التوثيق الإلكتروني، وذلك في ضوء تولي الأخيرة لمهام تقديم الخدمات الأمنية للبنك وعملائه على شبكة الإنترنت؛ وذلك من خلال التعرض لأهم الالتزامات القانونية الواقعة على عاتقها في مواجهة البنك، ومسؤوليتها عن الإخلال بها، في ضوء أهمية أمن البنك وتعاملاته المصرفية، وفى ضوء طبيعة المخاطر التي تهدده.

التوصيات

١- نوصي المشرع بأن يدرك الأهمية القصوى للبنك الإلكتروني على شبكة الإنترنت، وذلك بسبب التنامي المستمر لحركة التجارة الإلكترونية على شبكة الإنترنت، وما يقدمه هذا البنك من خدمات لا غنى عنها لهذه التجارة والمتعاملين فيها، وذلك من خلال تبنى تشريع يحكم وينظم عمل هذا البنك، وذلك على النحو التالي:

(أ) أن يحرص المشرع على قصر ممارسة العمليات المصرفية على شبكة الإنترنت على البنوك فقط، وذلك في ضوء ما تتميز به هذه العمليات من أهمية كبيرة في الحياة الاقتصادية بصورة عامة، على النحو الذي يفضل معه عدم السماح لغير البنك بالاشتغال بها، نظرا لتمتعه دون غيره بضمانات تشريعية ورقابية تؤهله لمثل هذه العمليات.

(ب) رسم إطار قانوني واضح يحكم وينظم العلاقة بين البنك ومقدمي الخدمات الإلكترونية، ينطوي على معالجة صريحة للالتزامات الجوهرية في علاقة كل منهما بالآخر، خاصة من قبل مقدمي الخدمات الإلكترونية، الذين يجب أن يحرص المشرع على إلزامهم بالحصول على التراخيص التي تسمح لهم بتقديم الخدمات الإلكترونية التي تتناسب مع طبيعة العمل المصرفي. أيضا الحرص على التشديد من مسؤولياتهم في ضوء أهمية الأعمال التي يقدمونها للبنك.

(ج)صياغة نصوص قانونية تنظم قواعد تأسيس البنك الإلكتروني وتشغيله على شبكة الإنترنت، على أن تراعى هذه النصوص توافر كافة المقومات المالية والتشغيلية والأمنية والتقنية التي تؤهله للعمل المصرفي على شبكة

الإنترنت.

(د) استحداث نصوص قانونية خاصة للتعاقد المصرفي على شبكة الإنترنت، بحيث تراعى خصوصيات التعاقد المصرفي، وتراعى الطبيعة الإلكترونية لوسيلة التعاقد، وما يتطلبه ذلك من إجراءات للتوثيق والتعريف بأطراف المعاملة، خاصة التعرف على شخصية العميل وضماناته المالية التي تؤهله للحصول على الخدمة. أيضا التزام البنك بتزويد عميله بكافة البيانات الخاصة بالخدمة المصرفية، وإجراءات التعاقد الخاصة بها.

(ه) إفراد نصوص خاصة لتنظيم العمليات المصرفية المستحدثة في نظام عمل البنك الإلكتروني على شبكة الإنترنت؛ كإصدار النقود الإلكترونية والتحويل الإلكتروني للنقود، وغيرها من المعاملات التي ظهرت نتيجة عمل البنك على شبكة الإنترنت.

(و) تبنى مفهوم موسع لنطاق البيانات التي تعد من الأسرار المصرفية، ويجب صياغة نصوص خاصة لحماية سرية هذه البيانات من قبل كل من له سلطة في الاطلاع عليها، سواء من العاملين لدى البنك أم من مقدمي الخدمات الإلكترونية، أم من قبل جهة التوثيق الإلكتروني.

(ز) التشديد من مسؤولية البنك المدنية عن الإخلالات الأمنية التي تقع نتيجة لتقصيره في الاستعانة بالنظم الأمنية التي تكفل أمن المعاملات التي تتم عبر موقعه، وذلك على النحو الذي يدفعه إلى التزود بأفضل الأجهزة والبرامج الأمنية التي تكفل تأمين وجوده ومعاملاته على شبكة الإنترنت.

(ح)تبنى مفهوم خاص للتوثيق الإلكتروني في نظام عمل البنك على شبكة

الإنترنت، وذلك على النحو الذي يجعل خدمات التوثيق ملائمة للطبيعة الخاصة بالاعتداءات التي تستهدف وجود البنك ومعاملاته المصرفية على شبكة الإنترنت.

(ط)صياغة نصوص عقابية تتصدى لكافة صور الاعتداءات التي تستهدف أمن البنك ومعاملاته المصرفية، بحيث تتلاءم والطبيعة الخاصة لهذه الاعتداءات، مع إفراد عقوبات خاصة لها، وذلك بدلا من ثني عنق النصوص القائمة على نحو لا يليق بالسياسة الجنائية التي ترفض القياس.

٢- نوصى البنك المركزي بتبني نظم رقابية منظمة وقوية، تراعى طبيعة المخاطر التي تحيط بنظام عمل البنك الإلكتروني على شبكة الإنترنت، ومن خلال الاستعانة بالفنيين المتخصصين والمؤهلين للرقابة على نشاط هذا البنك بالنظر إلى الطبيعة التقنية الغالبة على نشاطه. كما يجب على جهة الرقابة أن تراعى عدم إثقال كاهل البنك بشروط ومعايير تقيد من حرية حركته، وتفقده القدرة على المنافسة العالمية.

٣- نوصى الحكومة المصرية بأن تتبنى سياسات وإستراتيجيات جديدة لتهيئة المناخ العام على تشجيع عمل البنك الإلكتروني على شبكة الإنترنت، وذلك من خلال ما يلي:

(أ) حث الجهات المعنية (الوزارات، الهيئات الحكومية) على إنشاء إدارات حكومية تختص فقط بشؤون التجارة الإلكترونية ومعاملاتها المختلفة، وخاصة البنوك العاملة عبر شبكة الإنترنت، وذلك لتراعى الطبيعة الخاصة لعمل هذه البنوك، ومن ثم تأتى إجراءاتها ملائمة لهذه الطبيعة.

كما يجب أن تسعى الحكومة إلى إنشاء مراكز تعليم وتدريب للعاملين في هذه البنوك، بحيث تؤهلهم على العمل المصرفي عبر شبكة الإنترنت، وتحيطهم علما بالتنظيم القانوني الذي يحكم عمل هذه البنوك، خاصة ما يتعلق بأهمية وخطورة البيانات المصرفية، وما يتطلبه ذلك من التزامات المحافظة على سريتها وسلامتها.

(ب) على الحكومة المصرية أن تسعى جاهدة في المحافل الدولية من أجل وضع اتفاقيات دولية لإيجاد تنظيم قانوني موحد للأنشطة الدولية للبنك الإلكتروني على شبكة الإنترنت، خاصة ما تعلق منها بنظم الرقابة على عملها، وذلك على النحو الذي من شأنه تقليص المخاطر الناجمة عن دولية نشاط هذا البنك. أيضا ما يتعلق بمواجهة الجرائم الإلكترونية التي تستهدف أمن البنك وتعاملاته.

(ج) تنشيط وتشجيع الشركات العاملة في مجال الخدمات الأمنية الإلكترونية على ابتكار نظم أمنية قوية تناسب وطبيعة المعاملات المصرفية الإلكترونية على شبكة الإنترنت، وما تتميز به هذه المعاملات من خصوصية في الحفاظ على سريتها وخصوصيتها.

مشروع قانون البنوك الإلكترونية على شبكة الإنترنت

رغبة في محاولة استكمال الجانب التطبيقي من هذه الدراسة، وفي محاولة لتبصير المشرع المصري الذي لم تشهد أروقته حتى الآن مناقشات حول تنظيم قانوني خاص بالبنك الإلكتروني العامل على شبكة الإنترنت، فأننا نقترح هذا المشروع:

الفصل الأول

تعريفات وأحكام عامة

المادة (١)

في تطبيق هذا القانون يكون للمصطلحات التالية المعاني المخصصة بجوار كل منها:

١- **البنك:** هو البنك العامل عبر شبكة الإنترنت، وهو عبارة عن بنك يظهر في صورة موقع إلكتروني على شبكة الإنترنت يحتوى على كافة البرمجيات اللازمة للتعامل بصورة كاملة مع العملاء بخصوص الخدمات المصرفية وغيرها من الخدمات التسويقية، ويرخص له القانون بممارسة أنشطته في بيئة إلكترونية.

٢- **مقدم الخدمات الإلكترونية:** الشخص الطبيعي أو المعنوي الذي يقدم خدمات إلكترونية للبنك على شبكة الإنترنت كخدمة الدخول وتصميم الموقع واستضافته على شبكة الإنترنت.

٣- **جهة الرقابة:** هي الجهة التي يرخص لها القانون بالرقابة على إنشاء وتشغيل

البنوك في مصر(البنك المركزي).

٤- **العقد المصرفي على شبكة الإنترنت:** تلاقى الإيجاب والقبول الخاص لكل من البنك الإلكتروني والعميل عبر شبكة الإنترنت بهدف إنشاء رابطة عقدية أو تعديلها أو إلغائها فيما يتعلق بإجراء عمليات مصرفية إلكترونية.

٥- **أمن البنك العامل على شبكة الإنترنت:** عبارة عن تأمين وجود البنك على شبكة الإنترنت، وتأمين كافة الخدمات المصرفية التي يقدمها.

٦- **جهة التوثيق الإلكتروني:** هي الجهة المسئولة عن تأمين وجود البنك وتعاملاته على شبكة الإنترنت.

المادة (٢)

أ- تسرى أحكام هذا القانون على البنوك التي تقدم الخدمات المصرفية الإلكترونية لعملائها بصورة مستقلة عبر شبكة الإنترنت.

ب- تسرى على هذه البنوك أحكام قانون التجارة رقم ١٧ لسنة ١٩٩٩، وقانون البنك المركزي والرقابة على النقد رقم ٨٨ لسنة ٢٠٠٣، وذلك فيما لا يتعارض مع أحكام هذا القانون واللائحة الخاصة به.

ج- يراعى عند تطبيق أحكام هذا القانون قواعد العرف التجاري الدولي ذات العلاقة بالبنوك العاملة عبر شبكة الإنترنت.

د- تسرى أحكام هذا القانون على البنوك العاملة عبر شبكة الإنترنت، والتي تنشأ ويرخص لها وفقا لأحكام القانون المصري.

هـ- لا يسرى هذا القانون على البنوك التقليدية والتي تقدم خدمات مصرفية

إلكترونية.

الباب الأول

إنشاء البنك والرقابة عليه

الفصل الأول

إنشاء البنك على شبكة الانترنت

المادة (٣)

أ- يلتزم البنك بانتقاء أفضل أنواع الأجهزة اللازمة لتشغيله، وتبنى أفضل النظم الإلكترونية لإدارة الشبكات.

ب- يلتزم مورد الأجهزة بإعلام البنك بكافة الجوانب المتعلقة باستخدامها، ويستمر هذا الالتزام طوال مدة استخدام البنك للأجهزة ما لم يتم الاتفاق على غير ذلك.

ج- يسأل مورد الأجهزة عن المخاطر الناجمة عنها في مواجهة البنك والغير.

د- يسأل البنك في مواجهة العملاء بوصفه حارسا للأجهزة الإلكترونية الخاصة به، كما يسأل أيضا عن كافة الأضرار الناجمة عن عملها، ما لم يثبت السبب الأجنبي.

المادة (٤)

أ- يلتزم البنك بالحصول على ترخيص من صاحب الشأن إذا استغل البرامج المعلوماتية لصالح العملاء، ويلتزم بمراعاة الحدود المقررة كما ورد في عقد الترخيص.

ب- يلتزم البنك والعاملين لديه بالمحافظة على سرية البرامج المعلوماتية.

ج- يسأل البنك عن أي إخلال يقع على حقوق الملكية الفكرية المتعلقة بالبرامج المعلوماتية الخاصة بتشغيل البنك.

د- تنعقد مسؤولية البنك عما يقع من العاملين لديه من انتهاكات لحقوق الملكية الفكرية الخاصة بمؤلف البرنامج، ما لم يثبت البنك أنه لم يكن يعلم بمثل هذه الانتهاكات، وأنه قام فور علمه باتخاذ الإجراءات اللازمة لمنع ذلك.

يسأل مؤلف البرنامج المعلوماتي عن المخاطر الناجمة عنه في مواجهة البنك والغير المتضرر.

المادة (٥)

(أ) يلتزم مقدم الخدمة بتزويد البنك بكافة الأجهزة والموصلات اللازمة لاتصال البنك واستضافة موقعه على شبكة الإنترنت، وذلك بما يتلاءم مع طبيعة العمليات المصرفية، وحجم نشاط البنك.

(ب) يمتنع على مقدم الخدمة الاطلاع على البيانات المصرفية، ما لم تكن هناك ضرورة تبرر هذا الاطلاع، على أن تقدر الضرورة بقدرها.

(ج) يعامل مقدم الخدمة معاملة البنك والعاملين لديه فيما يتعلق بالحفاظ على السرية المصرفية. كما يسأل مقدم الخدمة في مواجهة البنك عن أن تحريف يقع لرسائل البيانات المتبادلة بين البنك وعميله.

(د) يجب على البنك أن يحدد طبيعة البيانات التي يمكن لمقدمي الخدمة الاطلاع عليها، كما يجب أن يتبنى إجراءات رقابية صارمة على خدماتهم للبنك.

(ه) يسأل مقدم الخدمة في مواجهة البنك عن سلامة الأجهزة الإلكترونية المستخدمة ضد كافة أشكال المخاطر التي تسببها ما لم يثبت السبب الأجنبي.

(و) يسأل مقدم الخدمة في مواجهة عملاء البنك طبقا للقواعد العامة.

(ز) يلتزم البنك والعاملين لديه بعدم المساس بأي عمل موجود على الموقع الإلكتروني للبنك يكون للمصمم عليه حق بموجب قانون الملكية الفكرية.

(ح) يسأل مقدم الخدمة عن الاعتداءات التي تقع من الغير على أحد محتويات موقع البنك والمشمولة بالحماية كأحد عناصر الملكية الفكرية أو الصناعية، وذلك ما لم يثبت اتخاذه الإجراءات اللازمة لمنع المعتدى من الوصول إلى هذه العناصر.

الفصل الثاني

الرقابة على البنك العامل على شبكة الانترنت

المادة (٦)

أ) يتم إنشاء قسم خاص داخل البنك المركزي المصري للقيام بمهام الترخيص لإنشاء البنوك على شبكة الإنترنت، والرقابة على أنشطة هذه البنوك.

ب) يتم تسجيل أية منشأة ترغب في العمل كبنك على شبكة الإنترنت في مصر وفقا للأوضاع المقررة في قانون البنك المركزي والجهاز المصرفي والنقد رقم ٨٨ لسنة ٢٠٠٣ ولائحته التنفيذية، وذلك بالإضافة إلى الشروط التالية:

- أن يستوفى جميع الإجراءات الموضوعة التي تحددها اللائحة التنفيذية لهذا القانون سواء فيما يتعلق بالتصميم الفني لشبكة البنك، أو برامج المعلومات القائمة على تشغيل هذه الشبكة. ويجب أن يضمن البنك في أوراقه المقدمة رسما تخطيطيا وشرحا وافيا لكل العناصر الداخلة في تكوين هذه الشبكة، بما في ذلك المواقع الإلكترونية التي يوجد لها رابط على موقع البنك على شبكة الإنترنت والعقود التي تحكم علاقة البنك بأصحاب هذه المواقع، بالإضافة إلى العقود الخاصة بتأمين الشبكة الداخلية والموقع الإلكتروني للبنك على شبكة الإنترنت.

- يجب على البنك أن يستوفى جميع الإجراءات الموضوعة من قبل البنك المركزي، للمراجعة والموافقة على السياسة الائتمانية التي سوف ينتهجها البنك في تعاملاته مع العملاء عبر شبكة الإنترنت؛ بما في ذلك الأسلوب الذي يتبعه البنك في الإقراض، وأنواع القروض وحجمها، وأنواع الضمانات التي يتطلبها البنك من العملاء لمنح هذه القروض.

- يجب على البنك أن يقدم المستندات التي تفيد قيامه بتسجيل العنوان الإلكتروني والعلامة التجارية لدى الجهات المختصة.

- يجب على البنك أن يقدم ما يفيد استيفاءه لكل المتطلبات الأمنية، سواء فيما يتعلق بالأجهزة والأدوات التي من شأنها تأمين وجود البنك وتعاملاته، أم فيما يتعلق بالإجراءات التي يفرض البنك التعامل بها مع أجهزته من قبل كل من العاملين لديه أو المتعاملين معه. كذلك يجب أن يقدم ما يفيد اختبار تشغيل هذه الأجهزة من قبل مراجع فني متخصص في هذا المجال، ويجب على هذا المراجع أن يعد تقريرا مكتوبا، يدون

فيه أنواع التدابير الأمنية التي استعان بها البنك، بما في ذلك برامج الحماية، والإجراءات الخاصة بالتحكم والتأكد من البيانات الداخلة والخارجة، ونظم التحقق من شخصية المتعامل مع البنك، والإجراءات التي تكفل لهذا المتعامل الدخول الآمن على الموقع الإلكتروني للبنك والتعامل معه. ويملك البنك المركزي أن يبدى أي ملاحظات أو توصيات تتعلق بهذا الاستعداد الأمني.

- يجب على البنك أن يقدم نماذج للعقود الخاصة بمختلف الخدمات المصرفية التي يؤديها عبر شبكة الإنترنت، وذلك للنظر في مدى مراعاتها لقوانين حماية المستهلك الإلكتروني.

- يجب على البنك أن يقدم لمكتب الرقابة على النقد ما يفيد تأهيل الطاقم الإداري سواء على مستوى المدراء أم على مستوى العاملين.

- يجب على البنك أن يقدم صورة طبق الأصل من العقود التي تحكم علاقته بمزودي الخدمات الإلكترونية، وما يفيد تأهيلهم وحصولهم على التراخيص التي تسمح لهم تقديم هذه الخدمات.

- يجب على البنك أن يقدم خطة للرقابة الداخلية على مجمل نشاطه، سواء على مستوى العاملين لديه، أم على مستوى التعامل مع العملاء. ويجب أن تتضمن هذه الخطة على تخصيص إدارة تقوم على هذا الأمر وفق إجراءات دقيقة ومحكمة.

- يجب على البنك أن يعد خطة تشغيل احتياطية لمواجهة الطوارئ التي يمكن أن تحدث أثناء عمل البنك، والتي من شأنها أن تؤثر على انتظام

سير العمل المصرفي.

- إفصاح البنك عن كون القوانين المصرية هي التي تحكم الخدمات التي يقوم بتأديتها للعملاء عبر شبكة الإنترنت.

ج) يجب على البنك المركزي التأكد من استيفاء الشروط السابقة قبل أن يمنح الترخيص للبنك بالبدء في مباشرة نشاطه، وله أن يبدى الملاحظات والتوصيات،وله أن يؤخر إصدار القرار النهائي بالموافقة على الترخيص للبنك، حتى يتأكد تماما من أنجاز كل هذه الملاحظات والتوصيات كما طلب، فأن لم يتم استيفاؤها فله أن يرفض طلب الترخيص.

د) للبنك المركزي أن يرفض الترخيص للبنك بالعمل على الرغم من استيفائه لكافة المتطلبات إذا ما اقتضت الظروف الاقتصادية للدولة ذلك.

ه) على البنك المركزي أن ينظم إجراءات رقابية تمارس بصورة دورية على نشاط البنك بعد الترخيص له بالإنشاء، وله أن يفرض على البنك متطلبات جديدة إذا ما دعت الحاجة لذلك، وله أن يقرر شطب تسجيل البنك إذا وقع إخلال بأحد الشروط السابقة.

و) يعمل بأحكام الباب السابع من أحكام قانون البنك المركزي والجهاز المصرفي والنقد رقم ٨٨ لسنة ٢٠٠٣ بشأن المخالفات التي تقع من البنوك العاملة عبر شبكة الإنترنت.

الباب الثاني

العقود المصرفية على شبكة الإنترنت

الفصل الأول

قواعد إبرام العقود المصرفية على شبكة الانترنت

المادة (٧)

أ) تخضع العقود المصرفية على شبكة الإنترنت للقواعد العامة التي تحكم العقود التجارية والمدنية، من حيث صحتها، وحجيتها، وقابليتها للتنفيذ، فيما لا يتعارض وأحكام هذا القانون.

ب) ينعقد العقد المصرفي على شبكة الإنترنت باستخدام رسائل البيانات مادامت قاطعة الدلالة في التعبير عن الإرادة.

ج) يلتزم البنك بالإفصاح عن اللغة التي يتم بها التعاقد معه عبر شبكة الإنترنت، كما يجوز للبنك أن يحدد النطاق المكاني للإيجاب الصادر عنه.

د) العرض الصادر عن البنك سواء كان عاما أم خاصا لإبرام عقد مصرفي عبر شبكة الإنترنت يعتبر مجرد دعوة للتعاقد، ما لم تتجه إرادة البنك بصورة صريحة إلى اعتباره إيجابا ملزما.

ه) ينعقد العقد المصرفي على شبكة الإنترنت في اللحظة التي يعلم فيها المتعاقد بالرسالة المتضمنة لقبول البنك، ويفترض أن المتعاقد قد علم بهذه الرسالة من لحظة وصولها إليه، ما لم يثبت عكس ذلك.

و) يلتزم البنك بتمكين العميل من العدول عن العقد المصرفي بعد إبرامه خلال مدة لا تقل عن سبعة أيام من تاريخ انعقاد العقد، وذلك متى أعلن العميل البنك عن رغبته في الانسحاب خلال هذه المدة، ومادام لم يكتمل أداء كل منهما تجاه الآخر.

ز) يلتزم البنك بوضع التعليمات والإرشادات الخاصة بكيفية التعامل مع موقعه الإلكتروني له، بالإضافة إلى كافة البيانات الخاصة بكل خدمة مصرفية يقدمها، وكيفية التعاقد معه بخصوصها في مكان واضح ومناسب، ومن أهمها:

- كافة البيانات الخاصة بالتعريف بالبنك وكشف هويته، كعلامته التجارية ورقم تسجيله (سجل تجارى)، ورقم قيده لدى جهة الرقابة.
- السياسة الأمنية التي تحكم استعمال موقع البنك والتعامل معه، وتحديد مسؤوليات العميل بخصوصها.
- السياسة التي تحكم الحفاظ على سرية البيانات الخاصة بالمعاملات المصرفية التي تتم عبر موقع البنك، وذلك من خلال:
- الخطوات الفنية المختلفة اللازمة لإبرام العقد المصرفي عبر شبكة الإنترنت، بداية من كيفية التوصل لنموذج العقد الموجود على موقع البنك والذي يحكم تقديم الخدمة المصرفية، والكيفية التي يمكن من خلالها التعرف على بنود العقد وشروطه، والطريقة التي يمكن من خلالها للعميل أن يعبر عن إرادته للالتزام بهذا العقد.
- كافة الوسائل الإلكترونية المتاحة التي من خلالها يستطيع العميل

تصحيح أي خطأ يتعلق بأى بيان من البيانات المدخلة أثناء التعاقد.

- بنود العقد والشروط العامة في شكل نموذجي، على نحو يسمح للعميل أن ينقل هذه الشروط ويخزنها.

- الخطوات الفنية الواجب على العميل القيام بها لتأمين إرسال البيانات الخاصة بالتعاقد، ككيفية وضع الشفرة الخاصة بأي معاملة مع البنك، بصورة إلكترونية وأي معلومات متعلقة بهذا.

ح) يلتزم البنك عند قيامه بتجميع البيانات اللازمة للتعاقد من عميله مراعاة ما يلي:

- أن يتم تجميع هذه البيانات وفقا لأغراض واضحة ومحددة، وأن يتم التعامل معها وفقا لهذه الأغراض.

- أن تكون هذه البيانات كافية وذات صلة بالغرض الذي تم التجميع من أجله، بحيث لا يطلب من العميل بيانات أكثر مما يلزم، وإن حدث هذا يجب حذف البيانات الزائدة.

- يجب اتخاذ الإجراءات اللازمة للتأكد من صحة هذه البيانات، والتأكد من أن هذه البيانات سارية حتى تاريخ التعاقد.

- يجب أن يتم وضع نموذج العقد بطريقة تسمح بتوضيح البيانات المطلوب من العميل ذكرها. ويجب الحفاظ على سلامة هذه البيانات، وذلك من خلال تأمين عملية إدخال هذه البيانات، وكذلك تخزينها.

ط) يلتزم البنك والعاملين لديه بالحفاظ على سرية كافة البيانات التي يحصل

عليها من العملاء، ويسأل البنك عن كافة الأضرار التي تلحق العميل من جراء ذلك، ما لم يثبت البنك السبب الأجنبي.

ي) ما لم يتم الاتفاق على غير ذلك، يخضع العقد المصرفي عبر شبكة الإنترنت للقانون المصري مادامت مصر هي الموطن المشترك للبنك والعميل، أيضا يسرى القانون المصري في حالة اختلاف الموطن، مادام موطن البنك في مصر.

الفصل الثاني

أحكام المسئولية المصرفية

المادة (٨)

أ) يجوز للبنك أن يقدم لعملائه خدمات فنية مادامت ضرورية لممارسة العمليات المصرفية على شبكة الإنترنت.

ب) مع عدم الإخلال بما ورد في المادة (٧) يجوز للبنك أن يقدم جميع الخدمات المصرفية على شبكة الإنترنت.

ج) للبنك أن يزود العميل بكافة الأجهزة الإلكترونية والبرامج اللازمة للتعامل المصرفي عبر شبكة الإنترنت، مع إحاطته علما بكافة الجوانب الفنية والأمنية والقانونية المتعلقة باستعمال هذه الأدوات.

د) يلتزم البنك بتمكين عملائه من الاستفادة من الخدمات المصرفية التي يقدمها للغير، بما في ذلك من توفير الأدوات الإلكترونية وتهيئتها لهذا الغير.

هـ) يسأل البنك في مواجهة العميل عن كافة الأضرار التي تلحقه نتيجة سوء عمل الأدوات الإلكترونية، كما يسأل عن كافة الأضرار الناتجة عن أعطال هذه الأدوات، ما لم يثبت أن سبب العطل إهمال العميل في اتباع التعليمات الخاصة باستعمالها.

و) يلتزم العميل بإخطار البنك بأسرع ما يمكن بكافة ما يمنعه من استعمال الأدوات الإلكترونية الخاصة بتعامله مع البنك، سواء لعطل فيها أم لفقدها.

ز) يتحمل العميل المسؤولية عن الخسائر التي تقع بسبب تأخره في إخطار البنك

بما يمنعه من استعمال الأدوات الإلكترونية الخاصة بتعامله مع البنك، ما لم يثبت خطأ البنك في ذلك. كما يتحمل البنك المسؤولية عن الأضرار التي تقع للعميل بعد قيامه بهذا الإخطار، ما لم يثبت البنك السبب الأجنبي.

ح) يلتزم العميل بالمحافظة على سلامة الأدوات الإلكترونية المسلمة له من البنك، بما في ذلك مراعاة التعليمات الخاصة باستعمالها، والحفاظ على سرية البيانات الخاصة باستعمالها. كما يلتزم العميل برد هذه الأدوات في نهاية العقد سواء كانت نهاية طبيعية بانتهاء مدته، أم كانت نهاية مبتسرة بالفسخ أو غلق الحساب أو غير ذلك من الأسباب.

ط) لا يخل هذا القانون بالاتفاقات الدولية المتعلقة بالمعاملة الضريبية المبرمة بين مصر والدول الأجنبية والمنظمات الدولية.

الباب الثالث

أمن البنك الإلكتروني على شبكة الإنترنت

الفصل الأول

الإلتزامات الأمنية للبنك على الانترنت

المادة (٩)

أ- يلتزم البنك باتخاذ كافة الاحتياطات الأمنية اللازمة لتأمين موقعه الإلكتروني، وتعاملاته المصرفية عبر شبكة الإنترنت، مراعيا في ذلك طبيعة محل الحماية والبيئة التي يعمل فيها.

ب- يلتزم البنك بالنص في كافة العقود المصرفية على تعليمات الأمن التي يجب على العميل التقيد بها أثناء تعامله مع البنك.

ج- تنتفي مسؤولية البنك عن الإخلالات الأمنية إذا أثبت إهمال وتقصير العميل في اتباع تعليمات الأمن.

د- يلتزم البنك بالتعاقد مع إحدى جهات التوثيق الإلكتروني على تقديم خدمات التأمين الإلكتروني للبنك وعملائه عبر شبكة الإنترنت.

الفصل الثاني

الالتزامات الأمنية لجهة التوثيق الالكترونى

المادة (١٠)

أ- تلتزم جهة التوثيق بتأمين موقع البنك وتعاملاته المصرفية. وليس مجرد بذل

العناية في ذلك، ويقع باطلا كل شرط يرد في العقد بين البنك وجهة التوثيق يعفى الأخيرة من مسؤوليتها عن الاخلالات الأمنية التي تقع بسبب نشاطها.

ب- تلتزم جهة التوثيق بتزويد البنك بكافة الأجهزة والبرامج اللازمة لتأمينه بما يتلاءم مع طبيعة الخدمات المصرفية، وحجم تعاملات البنك على شبكة الإنترنت، وتضبط المعطيات التقنية المتعلقة بهذه الأدوات والوثوق بها بقرار من وزير الاتصالات.

ج- تسأل جهة التوثيق في مواجهة البنك عن سلامة الأجهزة والبرامج المسئولة عن تأمين معاملاته، ما لم تثبت جهة التوثيق خطأ البنك. كما تسأل جهة التوثيق بوصفها حارس عما تسببه الأجهزة الإلكترونية التي توجد تحت سيطرتها من أضرار للبنك وعملائه.

د- تلتزم جهة التوثيق بأن توضح للبنك الإجراءات التي يجب أن يتبعها في حالة وجود أي خلل أو عطل أو غيرها من الظروف التي من شأنها أن تورث الشك في مدى الأمان والمصداقية التي تتمتع بها الأجهزة والبرامج الأمنية، والوسيلة التي يمكن أن يتم بها هذا الإبلاغ، والمواعيد التي يمكن أن يتم فيها.

ه-تلتزم جهة التوثيق بالمحافظة على سرية البيانات التي تصل إليها من البنك وعملائه بمناسبة تقديم خدمات التوثيق، ويجب أن تتعامل مع هذه البيانات وفقا للمعايير التالية:

- حظر الدخول على البيانات المحفوظة الخاصة بالبنك إلا من قبل الأشخاص المخول لهم ذلك فقط.

- الاطلاع على هذه البيانات يكون لأغراض التوثيق فقط.
- يجب اتباع إجراءات مشددة لحفظ شهادات التوثيق والبيانات الخاصة بأصحابها.

و- تعامل جهة التوثيق فيما يصل إلى علمها من بيانات بحكم عملها معاملة البنك والعاملين لديه فيما يتعلق بالحفاظ على السر المصرفي.

ز- تلتزم جهة التوثيق بالمحافظة على سلامة رسائل البيانات المتبادلة بين البنك وعملائه، وتسأل عن أي تحريف بالتعديل أو التغيير أو الإضافة يطرأ على هذه الرسائل، ما لم تثبت السبب الأجنبي.

ح- تصدر جهة التوثيق شهادات توثيق للبنك وعملائه تستجيب لمقتضات السلامة والوثوق بما يتناسب وطبيعة المعاملات المصرفية على شبكة الإنترنت، ووفقا للمواصفات المحددة من الوزير المختص.

ط- تلتزم جهة التوثيق باتباع إجراءات دقيقة أثناء الحصول على البيانات الخاصة بعميل البنك والتأكد من صحتها، مراعية التأكد من البيانات اللازمة للحصول على الخدمة المصرفية، وذلك قبل إصدار شهادة التوثيق له، كما تلتزم بعدم إدخال أي تعديلات أو إضافات على هذه البيانات، ولها أن تحصل عليها من قبل الغير بعد الحصول على الموافقة الكتابية من طالب الشهادة. لكن يمتنع على جهة التوثيق جمع أية معلومات غير ضرورية لإصدار الشهادة. ويحظر عليها أيضا جمع أية معلومات خارج نطاق عملية التوثيق، ما لم تحصل على موافقة كتابية من العميل بذلك.

ي- تضمن جهة التوثيق صحة المعلومات الواردة في الشهادة، وذلك من تاريخ

تسليم الشهادة للبنك وعميله، كما تضمن أيضا الصلة بين صاحب الشهادة والتوقيع الإلكتروني الخاص به.

ك- تسأل جهة التوثيق عن كل ضرر لحق البنك أو أحد عملائه بسبب نشاط في تأمين المعاملات المصرفية، ما لم تثبت السبب الأجنبي.

الباب الرابع

العقوبات

المادة (١٢)

يعاقب بالحبس والغرامة التي لا تقل عن ١٠٠٠٠٠ مصري كل من عطل عمدا اتصال البنك بعملائه عبر شبكة الإنترنت بأي صورة من الصور.

المادة (١٣)

يعاقب بالحبس والغرامة التي لا تقل عن ١٠٠٠٠٠ مصري كل من دخل أو اتصل بطريقة غير مشروعة بأحد أجهزة البنك، أو قاعدة البيانات الخاصة به. وإذا تسبب هذا الدخول أو الاتصال في تحريف البيانات الموجودة بالحذف أو الإضافة أو التغيير يعاقب بالحبس مدة لا تقل عن سنة وغرامة لا تقل عن ٢٠٠٠٠٠ جنيه مصري.

المادة (١٤)

يعاقب بالسجن والغرامة التي لا تقل ٢٠٠٠٠ مصري كل من دخل على أحد الأجهزة الإلكترونية للبنك وتوصل بنية الغش إلى الاستيلاء على البيانات الخاصة بالبنك أو العملاء، أو حصل على مبالغ نقدية أو تسهيلات ائتمانية بدون وجه حق.

المادة (١٥)

يعاقب على الشروع في ارتكاب الجرائم المشار إليها المواد ١٢، ١٣، ١٤ بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على ٢٠٠٠٠.

المادة (١٦)

يعاقب بعقوبة إفشاء السر المصرفي كل مقدم خدمة إلكترونية أفشى سرية البيانات التي أطلع عليها بحكم طبيعة عمله لدى البنك. كما يعاقب كل مقدم خدمة أؤتمن على بيانات خاصة بالبنك أو عملائه وقام باستغلالها بطريقة غير مشروعة.

المادة (١٧)

يعاقب بعقوبة التزوير كل من اصطنع أو أملى بيانات كاذبة للتعامل مع البنك عبر شبكة الإنترنت. كما يعاقب بذات العقوبة كل من أنتحل شخصية أحد العملاء باستعمال توقيعه الإلكتروني أو أحد بياناته الشخصية التي يتعامل بها مع البنك.

المادة (١٨)

يجوز للمحكمة بعد الحكم على أحد الفاعلين في الجرائم السابقة، أن تقضى باتخاذ أحد التدابير التالية:

- مصادرة الأشياء المستخدمة في ارتكاب الجريمة.
- غلق الأماكن التي استخدمت في ارتكاب هذه الجرائم.

المادة (١٩)

مع عدم الإخلال بحكم المادة ٢١٧ من قانون العقوبات المصري، تختص المحكمة التي يقع في دائرتها المقر القانوني للبنك (مكان تواجد الخوادم الإلكترونية) بكافة الجرائم التي تقع ضده.

الباب الخامس

أحكام أنتقالية وختامية

المادة (٢٠)

تلتزم جميع الجهات المخاطبة بهذا القانون والعاملة قبل إصداره بتوفيق أوضاعها طبقا لما جاء فيه من أحكام خلال ثلاثة أشهر من تاريخ صدور لائحته التنفيذية.

المادة (٢١)

يسرى هذا القانون على كافة الدعاوى المتعلقة بالبنوك العاملة عبر شبكة الإنترنت، والتي لم يصدر فيها حكم نهائي بات حتى تاريخ نفاذ هذا القانون.

المادة (٢٢)

يعمل بهذا القانون بعد ثلاثين يوما من تاريخ نشره في الجريدة الرسمية، على جميع الجهات المختصة تنفيذ أحكامه كل فيما يخصه.

قائمة المختصرات

١.	**ACH**	Automated Clearing House
٢.	**AES**	Advanced Encryption Standard
٣.	**ATM**	Automated Teller Machine
٤.	**ATM Cards**	Automated Teller Machine Cards
٥.	BITS	Banking Industry Technology Secretariat
٦.	CA	Court of Appeal
٧.	**CHIPS**	The Clearing House Interbank Payments
٨.	**CLSR**	Computer law and security report
٩.	**CPS**	Certification Practice Statement
١٠.	**CPSS**	committee on payment and settlement system
١١.	**CPU**	Central processing unit of control of a P.C which executes programs

١٢.	**DES**	Data Encryption standard
١٣.	**DMCA**	The Digital Millennium Copyright Act
١٤.	**DPA**	Data Protection Act
١٥.	**E-banking**	Electronic Banking
١٦.	**EBG**	Electronic Banking Group
١٧.	**ECB**	European central bank
١٨.	**EFT**	Electronic Fund Transfer
١٩.	**EFTA**	Electronic Fund Transfer Act
٢٠.	**EGL**	Electronic Journal of Law
٢١.	**EP**	European parliament
٢٢.	**FAST**	federal agency safety transaction
٢٣.	**FFIEC**	Federal Financial Institutions Examination Council
٢٤.	**FIP**	The Code of Fair Information Practices
٢٥.	**FTC**	Federal trade center

٢٦.	FTP	file transfer protocol
٢٧.	GHSS	Journal of the Humanities& Social Sciences
٢٨.	GLB act	Gramm-Leach-Bliley Act
٢٩.	HTML	Hyper Text Markup Language
٣٠.	HTTP	Hypertext transfer Protocol
٣١.	IGIM	International Journal of Information Management
٣٢.	IOSCO	International Organization of securities commission
٣٣.	ISDN	Integrated Services Digital Network
٣٤.	ISP	Internet Service Provider
٣٥.	IT	Information Technology
٣٦.	JI	journal on the internet
٣٧.	JIBC	journal of Internet Banking and commerce
٣٨.	JILT	Journal of Information, Law and Technology
٣٩.	LAN	Local area network

٤٠.	**NACHA**	National Automated Clearing House Association
٤١.	**NIC**	Network Interface Card
٤٢.	**OCC**	Office of the Comptroller of the Currency
٤٣.	**OJEC**	Official journal of the European Communities
٤٤.	**OPPA**	Online Privacy Protection Act
٤٥.	**OSC**	Federal Reserve Board Official Staff Commentary
٤٦.	**Pc-banking**	PC-based E-banking
٤٧.	**PIN**	Personal identification number
٤٨.	**PKI**	public key infrastructure
٤٩.	**POS**	point of sale
٥٠.	**SEAL**	Digital Signature and Electronic Authentication Law
٥١.	**SNA**	Systems Network Architecture
٥٢.	**SWIFT**	Society for Worldwide Interbank Financial Telecommunications

٥٣.	**TCPL/IP**	Transmission control protol/internet protocol
٥٤.	**Texas Int, il. J**	Texas International Law Jourrnal
٥٥.	**UCC**	Uniform Commercial Code
٥٦.	**UCITA**	Uniform Computer Information Transaction
٥٧.	**UNICTRAL**	United nations commission on international trade law
٥٨.	**VAN**	Value added Network
٥٩.	**Web**	WORLD WIDE WEB

شرح المصطلحات الفنية

(A)

١. Applet

هو عبارة عن برنامج صغير يتم إلحاقه بأحد التطبيقات وذلك مثل متصفح البحث(web browser)، حيث يعمل هذا البرنامج على مساعدة التطبيق في العمل وأداء وظائفه.

(B)

١. Bandwidth

هو مصطلح يستخدم للتعبير عن كمية البيانات التي يمكن إرسالها عبر كابل توصيل لشبكة الإنترنت، وكذلك السرعة وطول الموجة التي يمكن أن تسيير بها هذه البيانات.

٢. Browser

وهو عبارة عن برنامج يستخدم في تصفح محتويات الوثائق والملفات الموجودة على الموقع وتحميلها.

(C)

١. Cryptography

الكتابة المشفرة عبارة عن وسيلة لحفظ الاتصالات سرية باستخدام التشفير،

حيث يتم من خلاله تحويل البيانات إلى صورة غير مفهومة. التشفير وحل التشفير يحتاج عادة إلى استخدام بيانات معينة تسمى (مفتاح التشفير).

(D)

١. DES

هو معيار لتشفير البيانات (The Date Encryption Standard)، يستخدم كخوارزمية للتشفير، وقد اعتمد من قبل المعهد الـوطني الأمريكـي للمعـايير والتقنية (NIST)، والمعهد القومي للمعايير الأمريكي (ANSI)، وذلك كمعيـار أمن يستخدم لتشفير البيانات الهامة.

(F)

١. Firewall

الحائط الناري، هو عبارة عن مجموعة من الأجهزة والبرامج، أو نظام يقع بين شبكة الإنترنت والشبكة الخاصة المراد حمايتها، وذلك من حـزم البيانـات المارة من الخارج إلى الداخل، والعكس (البيانات المارة من الداخل إلى الخارج)، وذلك للتأكد من أن البيانات المارة مسموح لها بالمرور وفقا للسياسة الأمنية التي تحكم تشغيل الشبكة الخاصة.

٢. FTP

هو عبارة عن بروتوكول لنقل الملفات، حيث يقوم بنقل واسـتلام الملفـات عبر شبكة الإنترنت.

(H)

١. HTML (Hypertext mark-up language)

هو عبارة عن اللغة المستخدمة لإنشاء وتصميم النـصوص عنـى شـبكة الإنترنت، وذلك من خلال أكواد معينة تعمل على تصنيف عناصر النص وربط بعضها ببعض.

٢. HTTP

وهو عبارة عن بروتوكول يستخدم لنقل ملفات (HTML) فيما بين المتصفح (Browsers) ومقدم الخدمة (web servers).

٣. Hypertext

هو عبارة عن اتصال كلمة أو عبارة بنقطة أخرى في ذات صفحة الويب المعروضة أو في صفحة أخرى، بحيث يمكن الوصول إلى النقطة الأخرى بمجرد الضغط على هذه الكلمة أو العبارة.

(I)

١. IP

وهو اختصار يشير إلى البروتوكول الخاص بعمل شبكة الإنترنت (Internet protocol). ويعد هذا البروتوكول من أهم البروتوكولات التي يقوم عليها نظام عمل شبكة الإنترنت؛ حيث يتحكم في تحديد كيفية أنتقال حزم البيانات من مصدرها إلى المكان المتجهة إليه.

٢. (ISDN)

وهو اختصار يشير إلى شبكة الخطوط الرقمية المجمعة (Integrated Services Digital Network)، حيث تعمل هذه الشبكة على زيادة سرعة نقل البيانات عبر شبكة الإنترنت، أو عبر شبكة اتصال محلية عن بعد، خاصة إذا تعلق الأمر بملفات ذات حجم كبير مثل الصوت والصورة. وتصل السرعة في الشبكات المحلية منها إلى ١٢٨ بايت في الثانية، كما يمكن أن تزيد هذه السرعة

في حالة وجود خطوط تجارية (Commercial Link).

(P)

١. Packet

هي عبارة عن بيانات مجمعة بشكل يسمح بنقلها عبر شبكة رقمية، وتتكون الحزمة من مجموعة من البيتات bits، يتم تنظيمها بشكل منظم.

٢. PIN

ويشير اختصار (PIN) إلى رقم التعريف الشخصي (personal identification number)، وهو عبارة عن رقم مكون من مجموعة من الأعداد يستخدم للتعريف بشخص صاحبها. وهذه الأرقام شخصية، بحيث يجب على صاحبها أن يحرص دائما على سرية هذه الأرقام.

٣. Private Key

وهو مفتاح خاص يستخدم في التشفير وفك التشفير، وهو يعمل بالتزاوج مع مفتاح آخر يسمى المفتاح العام public key. ويتم الاحتفاظ بالمفتاح الخاص بصورة سرية من قبل مالكه.

٤. Protocol

هو عبارة عن طريقة أو أسلوب متفق عليه لتواصل اثنين أو أكثر من الأدوات العاملة على شبكة واحدة بطريقة إلكترونية، وذلك للاتصال فيما بينهم، وتنفيذ أوامر معينة.

٥. Public Key

يشير هذا المصطلح إلى المفتاح العام الذي يستخدم في التشفير أو فك التشفير، وهو يعمل بالتزاوج مع المفتاح الخاص (Private Key)، ويسمى المفتاح العام بسبب أنه معلوم للكافة، على عكس المفتاح الخاص الذي لا يعلمه إلا صاحبه.

(R)

١. RSA

وهو عبارة عن نظام من نظم التشفير غير المتماثل (asymmetric cryptography)، ويستخدم هذا النظام في التشفير والتوثيق، وقد تم اختراع هذا النظام عام ١٩٧٧ من قبل Ron Rivest، Adi Shamir، Leonard Adleman، ويعتمد هذا النظام على زوجين من المفاتيح للتشفير وفك التشفير.

(S)

١. Search engine

هو عبارة عن برنامج كمبيوتر يستخدم ككلمة دليلية (identification Key Word)، وذلك للبحث عن المواقع، وإنشاء خطوط اتصال فيما بينها.

٢. Server

وهو عبارة عن كمبيوتر مركزي يعمل على تزويد المستخدمين بما يحتاجون إليه من على هذا الكمبيوتر في وقت واحد.

(T)

١. TCP/IP (Transmission Control Protocol/Internet Protocol)

وهو يعد من أشهر البروتوكولات المستخدمة في شبكة الإنترنت، حيث يضم هذا البروتوكول مجموعة من القواعد التي تستخدم لإقامة وإنهاء الاتصالات،

وكذلك لتحديد مسار البيانات الصغيرة packets، وهناك نوع آخر من البروتوكولات يستخدم لنقل الملفات، ويسمى (FTP File Transfer Protocol) كما يوجد بروتوكول لنقل النصوص المتشعبة والمعلومات المتعددة الوسائط ويسمى

(http Hyper Text Transfer).

(W)

١. Web

هو مصطلح عام يشير إلى شبكة تضم مجموعة متشعبة من الحاسبات تكون مرتبطة فيما بينها بوصلات معينة تسمح بالتواصل بين هذه الحاسبات.

٢. Web pages

هو عبارة عن جهاز كمبيوتر متصل بشبكة الإنترنت، يعمل على تخزين الملفات، وعرضها على شبكة الإنترنت عبر محركات البحث.

قائمة المراجع

أولا: المراجع العربية:

(١)- المراجع العامة:

١- د. **أحمد السعيد الزقرد**، الوجيز في عقد الإيجار، (بدون دار للنشر)، ٢٠٠٠-٢٠٠١.

٢- د. **أحمد شوقي أبو خطوة**، الأحكام العامة لقانون العقوبات، النظرية العامة للجريمة (الجزء الأول)، دار النهضة العربية-القاهرة، ١٩٩٩.

٣- د. **أحمد شوقي عبد الرحمن**، النظرية العامة للالتزام (مصادر الالتزام)، دار القلم للنشر والتوزيع-المنصورة، ٢٠٠٠.

٤- د. **حسين الماحى**، أحكام الإفلاس في ظل قانون التجارة الجديد،دار النهضة العربية-القاهرة، ٢٠٠٢.

٥- د. **حمدي عبد المنعم**، العمليات المصرفية، دار النهضة العربية-القاهرة، الطبعة الأولى، (بدون تاريخ نشر).

٦- د. **عبد الرحمن السيد قرمان**، عمليات البنوك، دار النهضة العربية-القاهرة، الطبعة الثانية،٢٠٠٠.

٧- د. **عبد الفضيل محمد أحمد**، الأوراق التجارية وعمليات البنوك، دار النهضة العربية، (بدون تاريخ نشر).

٨- د. على البارودي، العقود وعمليات البنـوك التجاريـة، دار المطبوعـات الجامعية-الإسكندرية، ٢٠٠١.

٩- **د. على جمال الدين**، عمليات البنوك من الوجهة القانونية ،الطبعة الثالثـة، دار النهضة العربية-القاهرة.

١٠- **د. غنام محمد غنام**، الـوجيز فـي شـرح قـانون العقوبـات، القـسم الخاص،(بدون دار للنشر)، (بدون تاريخ نشر).

١١- **د. فتحي عبد الرحيم عبد الله**، الوجيز في النظرية العامة للالتزامات، مكتبة الجلاء الجديدة- المنصورة، الطبعة الثانية، ١٩٩٩.

١٢- **د. محسن عبد الحميد البيه**، النظرية العامـة للالتـزام (المـصادر غيـر الإرادية) دار النهضة العربية-القاهرة، ٢٠٠٨.

١٣- **د. محمد لبيب شنب**، أحكام عقد المقاولة، منشأة المعـارف-الاسـكندرية، الطبعة الثانية، ٢٠٠٤.

١٤- **د. محمد محمد هلالية**، الإفلاس، الطبعة الأولى، ١٤٣١- ٢٠١٠،(بـدون دار نشر).

١٥- **د. محمد ناجى ياقوت**، عقد المقاولة، (بدون دار نشر)، ٢٠٠٧.

(٢)- __الكتب المتخصصة:__

١- أ. **المنصف قرطاس**، دراسة تحليلية حول فرص الاستثمار في البنك المباشر أو الإنترنت البنكى، اتحاد المصارف العربية،٢٠٠٠.

٢- **توفيق شمبور**، مسائل قانونية خاصة بالتجارة الإلكترونية، مجموعة بحوث التجارة الإلكترونية والخدمات المصرفية والمالية عبر الانترنت، اتحاد المصارف العربية، ٢٠٠٠.

٣- **ج.س. شيشير – س.هـ. فيفوت – م.ب. فيرمستون**، أحكام العقد في القانون الإنجليزي، نقله من الإنجليزية إلى العربية هنري رياض، دار الجيل بيروت، مكتبة خليفة عطية الخرطوم، ١٩٧٦.

٤- **د. إبراهيم المنجى**، عقد نقل التكنولوجيا، منشأة المعارف، الطبعة الأولى، (٢٠٠٢).

٥- **د. أسامة أبو الحسن مجاهد**، خصوصية التعاقد عبر الإنترنت، دار النهضة العربية. ٢٠٠٣.

٦- **د. أسامة أحمد بدر**، حماية المستهلك في التعاقد الإلكتروني، دار الجامعة الجديدة للنشر، ٢٠٠٥.

٧- **د. السيد عتيق**، جرائم الإنترنت، دار النهضة العربية، ٢٠٠٢.

٨- **د. السيد محمد السيد عمران**، الطبيعة القانونية لعقود المعلومات، مؤسسة الثقافة الجامعية، الإسكندرية، ١٩٩٢.

٩- **د. ثروت عبد الحميد**، التوقيع الإلكتروني، مكتبة الجلاء الجديدة- المنصورة، ٢٠٠١.

١٠- **د. جمال عبد الرحمن محمد على**، الخطأ في مجال المعلوماتية، (بدون دار نشر). ٢٠٠٣.

١١- د. **جميل عبد الباقى الصغير**، القانون الجنائى والتكنولوجيا الحديثة، الكتاب الأول (الجرائم الناشئة عن استخدام الحاسب الآلى)، الطبعة الأولى، دار النهضة العربية، ١٩٩٢.

١٢- د. **حسن حسين البراوى**، عقد تقديم المشورة، دار النهضة العربية، ١٩٩٨.

١٣- د. **حسن عبد الرحمن قدوس**، مدى التزام المنتج بضمان السلامة في مواجهة مخاطر التطور العلمي، دار النهضة العربية-القاهرة، (بدون تاريخ نشر).

١٤- د. **خالد مصطفى فهمي**، الحماية القانونية لبرامج الحاسب الآلي ،دار الجامعة الجديدة للنشر، ٢٠٠٥.

١٥- د. **خالد ممدوح إبراهيم**. إبرام العقد الإلكتروني، دار الفكر الجامعى، ٢٠٠٦.

١٦- د. **خالد ممدوح إبراهيم**، حماية المستهلك في المعاملات الإلكترونية، الدار الجامعية، ٢٠٠٧.

١٧- د. **رأفت رضوان**، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، ١٩٩٨.

١٨- د. **سعد على أحمد رمضان**، المسؤولية المدنية الناشئة عن الإخلال بالالتزام بالسرية دراسة مقارنة بالفقه الإسلامى، دار النهضة العربية، ٢٠٠٧.

١٩- د. **سعيد سعد عبد السلام**، الالتزام بالإفصاح في العقود، دار النهضة العربية، الطبعة الأولى، ٢٠٠٠.

٢٠- د. **سعيد سعد عبد السلام**، الحماية القانونيــة لحــق المؤلــف والحقــوق المجاورة، دار النهضة العربية، ٢٠٠٤.

٢١- د. **سعيد عبد اللطيف حسن**، الحماية الجنائيــة للــسرية المــصرفية، دار النهضة العربية،٢٠٠٤.

٢٢- د. **سمير حامد الجمال**، التعاقد عبر تقنيات الاتصال الحديثة، دار النهــضة العربية، الطبعة الأولى، ٢٠٠٦.

٢٣- د. **شريف محمد غنام**، التنظيم القانوني للإعلانات التجارية عبــر شــبكة الإنترنت، (بدون دار نشر)، ٢٠٠٦.

٢٤- د. **شريف محمد غنام**، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوأن الإلكتروني، دار النهضة العربية-القاهرة، (بدون تاريخ نشر).

٢٥- د. **شريف محمد غنــام**، محفظة النقود الإلكترونية، دار النهضة العربيــة-القاهرة، (بدون تاريخ نشر).

٢٦- د. **شريف محمد غنام**، مسؤولية البنك عن أخطاء الكمبيــوتر فــي النقــل الإلكتروني للنقود، دار النهضة العربية-القاهرة، بدون تاريخ نشر.

٢٧- د. **صلاح الدين جمال الدين**، عقود نقل التكنولوجية، دار الفكر الجــامعي، ٢٠٠٥.

٢٨- د. **طارق طه**، إدارة البنوك في بيئة العولمــة والإنترنــت، دار الجامعــة الجديدة، ٢٠٠٧.

٢٩- د. **عادل أبو هشيمة محمود حوته**، عقود خدمات المعلومات الإلكترونية في

والمصارف العربية (الجزء الأول)، اتحاد المصارف العربية، ١٩٩٧.

(٣)- <u>رسائل الدكتوراه:</u>

١- **د.أحمد السيد لبيب**، الدفع بالنقود الإلكترونية، رسالة دكتوراه - كلية الحقوق - جامعة المنصورة،٢٠٠٧.

٢- **د.أنس السيد عطية سليمان**، الضمانات القانونية لنقل التكنولوجيا إلى الدول النامية والمشروعات التابعة لها، رسالة دكتوراه، كلية الحقوق- جامعة عين شمس، ١٩٩٦.

٣- **د.إيمان مأمون سليمان**، الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، ٢٠٠٥ -٢٠٠٦.

٤- **د.بشار طلال أحمد مومني**، مشكلات التعاقد عبر الإنترنت، رسالة دكتوراه كلية الحقوق - جامعة المنصورة، ٢٠٠٣م.

٥- **د.شيماء عبد الغنى محمد عطا الله**، الحماية الجنائية للمعاملات الإلكترونية، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، ٢٠٠٥م.

٦- **د.عزة محمود أحمد خليل**، مشكلات المسئولية المدنية في مواجهة فيروس الحاسب، رسالة دكتوراه، كلية الحقوق- جامعة القاهرة، ١٩٩٤.

٧- **د. عيسى غسان عبد الله الربضى**، القواعد الخاصة بالتوقيع الإلكتروني، رسالة دكتوراه، كلية الحقوق ــ جامعة عين شمس، ٢٠٠٦.

٨- **د.محمد أحمد محمد نور جستنية**، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق - جامعة القاهرة،

.٢٠٠٥

٩- د. **محمد سعيد إسماعيل**، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق – جامعة عين شمس، ١٤٤٦هـ – ٢٠٠٥م.

١٠- **د. محمد عبد الحي إبراهيم سلامة**، إفشاء السر المصرفي بين الحظر والإباحة، رسالة دكتوراه، كلية الحقوق ــ جامعة المنصورة، ٢٠٠٤.

١١-**د. محمد لبيب شنب**، المسئولية عن الأشياء (رسالة دكتوراه)، مكتبة النهضة المصرية، ١٩٥٧..

(٤)- أبحاث المؤتمرات:

١. د. **إبراهيم الدسوقي أبو الليل**، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المتضرر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون ،٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣م، غرفة تجارة وصناعة دبي.

٢. د. **أحمد الهوارى**، عقود التجارة الإلكترونية في القانون الدولى الخاص، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون ،٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣م، غرفة تجارة وصناعة دبي.

٣. د. **إسماعيل شاهين**، أمن المعلومات في الإنترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون- جامعة الإمارات العربية المتحدة، من ١- ٣ مايو ٢٠٠٠.

٤. د. **بلال عبد المطلب بدوى**، البنك الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون ،٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠ -١٢ مايو٢٠٠٣م ،غرفة تجارة وصناعة دبي.

٥. د. **ثناء أحمد محمد المغربي**، الوجهة القانونية لبطاقات الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي.

٦. د. **سعيد الحامز**. العمليات المصرفية الإلكترونية والإطار الإشرافي، مؤتمر

الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ ه ١٠-١٢ مايو ٢٠٠٣ دبي.

٧. د. **صفوت عبد السلام عوض الله**، الآثار الاقتصادية لعمليات غسيل الأموال ودور البنوك في مكافحة هذه العمليات، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون ،٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣م، غرفة تجارة وصناعة دبي.

٨. د. **عدنان إبراهيم سرحان**، الوفاء (الدفع) الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون،٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي.

٩. د. **غنام محمد غنام**، حدود المسؤولية الجنائية للمصارف المالية عن مخالفة واجب السرية وعن غسيل الأموال، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ ه ١٠-١٢ مايو ٢٠٠٣ دبي.

١٠. د. **فايز عبد الله الكندرى**، التعاقد عبر شبكة الإنترنت في القانون الكويتي، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون ،٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣م، غرفة تجارة وصناعة دبي.

١١. د. **محمد إبراهيم محمود الشافعي**، الآثار النقدية والاقتصادية والمالية للنقود الإلكترونية، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة

تجارة وصناعة دبي.

١٢. د. **محمد سعدو الجرف**، أثر استخدام النقود على الطلب على السلع والخدمات، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون ٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣م، غرفة تجارة وصناعة دبي.

١٣. د. **محمد عبد الرحيم سلطان العلماء**، جرائم الإنترنت والاحتساب عليها، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون (جامعة الإمارات العربية المتحدة)، ٢٠٠٠.

١٤. د. **محمد عبد السلام محمد**، جرائم غسيل الأموال إلكترونيا في ظل النظام العالمي الجديد للتجارة الحرة (العولمة)، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون ٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣م، غرفة تجارة وصناعة دبي.

١٥. د. **محمود سمير الشرقاوي**، مفهوم الأعمال المصرفية الإلكترونية وأهم تطبيقاتها، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون ٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣م، غرفة تجارة وصناعة دبي .

١٦. د. **مصطفى محمد عرجاوى**، الحماية المدنية لبرامج الكمبيوتر في القوانين الوضعية، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون (جامعة الإمارات العربية المتحدة)، ٢٠٠٠.

١٧. د. **ممدوح خليل البحر**، د. عدنان أحمد ولى العزاوى، بطاقات الائتمان والآثار القانونية المترتبة بموجبها، مؤتمر الأعمال المصرفية الإلكترونية

بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي.

١٨. د. منظور أحمد حاجى الأزهري، بطاقة السحب النقدي، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ هـ الموافق ١٠ -١٢ مايو ٢٠٠٣ م، غرفة تجارة وصناعة دبي.

١٩. **د. نورى حمد خاطر**، مسؤولية المصرف عن الأضرار الناشئة عن استخدام النظام الرقمي في العمليات المصرفية بين المسؤولية المدنية وفعل المباشرة والتسبب، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤ ه ١٠-١٢ مايو ٢٠٠٣ دبي.

٢٠. **د.عزت محمد على البحيرى**، القانون الواجب التطبيق على المعاملات الإلكترونية، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون،٩-١١ ربيع الأول ١٤٢٤هـ الموافق ١٠- ١٢ مايو ٢٠٠٣م، غرفة تجارة وصناعة دبي.

٢١. **د. محمد عبد الحليم عمر**، بطاقات الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ٩-١١ ربيع الأول ١٤٢٤هـ الموافق١٠ -١٢ مايو ٢٠٠٣م، غرفة تجارة وصناعة دبي.

٢٢. **المؤتمر الإقليمي العربي الإفريقي حول سلامة المبادلات والإمضاء الإلكتروني وهيكل المفتاح العمومى**، في نطاق الإعداد لفعاليات القمة العالمية لمجتمع المعلومات تونس ٢٠٠٥، متاح على العنوان التالي:

http://www.certification.tn/Conference/PKITunisia٢٠٠٥/index.

htm

(٥)-**أبحاث منشورة فى دوريات**

١. **د. السيد أحمد عبد الخالق**، البنوك والتجارة الإلكترونية، مجلة البحوث القانونية والاقتصادية-كلية الحقوق – جامعة المنصورة.

٢. **د. حسن مظفر الرزو**، الأمن المعلوماتى: معالجة قانونية أولية، مجلة الأمن والقانون، أكاديمية شرطة دبي، السنة الثانية عشرة، العدد الأول، يناير ٢٠٠٤.

٣. **د.حسين الماحى**، مسؤولية البنك عن رفض منح أو تقديم الائتمان للمشروعات، مجلة البحوث القانونية والاقتصادية، كلية الحقوق ـ جامعة المنصورة، العدد (١٨)، أكتوبر ١٩٩٥

٤. **د. حسين الماحى**، نظرات قانونية في التجارة الإلكترونية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد الحادي والثلاثين، أبريل ٢٠٠٢.

٥. **د. سهير محمود معتوق**، لجنة بازل وكفاءة الرقابة المصرفية، مجلة مصر المعاصرة العدد ٤٨٢، ٢٠٠٦.

٦. **د. عبد المنعم فرج الصدة**، عقد الإذعان، مجلة الأمن والقانون، كلية شرطة دبي ، السنة الرابعة،العدد الأول، ١٤١٦- ١٩٩٦.

٧. **د. فتحى عبد الرحيم عبد الله**. العناصر المكونة للعقد كمصدر للالتزام،

مجموعة البحوث القانونية والاقتصادية – كلية الحقوق – جامعة المنصورة، العدد (٧)، ١٩٧٨.

٨. **د. فريد عبد المعز فرج**، التعاقد بالإنترنت، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون – فرع دمنهور، العدد الثامن عشر، الجزء الأول ١٤٢٤هـ – ٢٠٠٣م.

٩. **د.محمود مختار أحمد بريرى**، إبرام عقود نقل التقنية وتحديد محلها، مجلة الأمن والقانون، كلية شرطة دبى، السنة الرابعة،العدد الأول، ١٤١٦- ١٩٩٦.

١٠. **د. نشأت الخميسي**، برامج التعامل مع الويب، التجارة الإلكترونية، أكاديمية السادات للعلوم الإدارية – سلسلة إصدارات البحوث الإدارية، الإصدار (٣)، ٢٠٠١.

١١. **د. هشام صلاح الدين زكى**، تأثير التجارة الإلكترونية على البنوك،، أكاديمية السادات للعلوم الإدارية- سلسلة إصدارات البحوث الإدارية (٣)، ٢٠٠١.

(٦)- مقالات على الإنترنت باللغة العربية:

١- د. إلياس الهاجرى، جرائم الإنترنت، ص١:

http://www.egovs.com/egovs_webo٢/news.php?main=٧&detailsid=٢٨

٢- مقالة بعنوان تحديات الأمن:

http://www.itep.ae/arabic/Education١Center/CommNet/net_security.asp

٣- أحمد الهاشمي، التشفير بالمفتاح المتناظر:

http://www.boosla.com/showArticle.php?Sec=Security&id=٣٥

٤- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، الدليل الإلكتروني للقانون العربي، (بدون تاريخ نشر)، ص ٣٠، متاح على العنوان الإلكتروني التالي:

www.arablawinfo.com

٥- الضوابط الرقابية للعمليات المصرفية الإلكترونية وإصدار وسائل دفع للنقود الإلكترونية، البنك المركزي المصري، الجلسة المنعقدة بتاريخ ٢٨ فبراير ٢٠٠٢، ص٢:

http://www.cbe.org.eg/public/Regulations٪٢٠of٪٢٠The٪٢٠Electronic٪٢٠Banking٪٢٠Operations.doc

٦- البنك المركزي المصري، التقرير السنوي، ٢٠٠٤/٢٠٠٥.

http://www.cbe.org.eg/public/Annual٪٢٠Report٪٢٠٢٠٠٥.pdf

٧- يونس عرب، مقالة بعنوان البنك الإلكتروني:

http://www.arablaw.org/Download/E-Banking.doc

٨- يونس عرب، التعاقد والدفع الإلكتروني تحديات النظامين الضريبي والجمركي، ورقة عمل مقدمة لبرنامج الندوات المتخصصة حول التجارة الإلكترونية – معهد التدريب والإصلاح القانوني- الخرطوم، ٢٠٠٢.

٩- يونس عرب، دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي،

منشورات اتحاد المصارف العربية - ٢٠٠٢.

١٠- يونس عرب، جرائم الكمبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢، المركز العربي للدراسات والبحوث الجنائية - أبو ظبي ١٠-١٢ /٢/٢٠٠٢، ص١٦ . أنظر العنوان التالي :
http://www.arablaw.org/Download/CyberCrimes_General.doc

ثانيا: الأحكام القضائية:

١- نقض مدني مصري ١٤ /٦/ ١٩٦٧، طعن رقم ٢٩٤، س ق ٣١، مجموعة أحكام محكمة النقض، س ١٨، القاعدة (١٩٢)، ص ١٢٦٦.

٢- نقض مدني مصري، ١٩/٦/١٩٦٩، طعن رقم ٣٢٣ س ق ٣٥، مجموعة أحكام النقض (الجزء الأول)، س ٢٠، فقرة ج، القاعدة (١٥٩)، ص ١٠١٧.

٣- نقض مدني مصري في ١٢ / ٣/ ١٩٧٤، طعن رقم ٣٩٦، س ق ٣٧، مجموعة أحكام النقض، س ٢٥، قاعدة (٨٠)، ص ٤٩٣.

٤- نقض مدني مصري، ١٥/١/١٩٨٩، طعن ١٧٨١، س ق ٥٦، مجموعة أحكام النقض (الجزء الأول)، س ٤٠، القاعدة (٣٢)، ص ١٤٥

٥- نقض مدني مصري، ١٧ /١٢/ ١٩٩٥، طعن ٥٥٤، س ق ٥٩، مجموعة أحكام النقض (الجزء الثاني)، قاعدة (٢٧٤)، ص ١٣٩٦.

ثالثا- القرارات الوزارية:

-قرار وزير الثقافة رقم ٨٢ لسنة ١٩٩٣ في شأن تنفيذ قانون حماية حق

المؤلف فيما يتعلق بمصنفات الحاسب الآلي، الوقائع المصرية، العدد ١٠٤، ٩ مايو ١٩٩٣.

رابعا- أهم القوانين:

أ- القوانين المصرية:

١- قانون رقم ٨٨ لسنة ٢٠٠٣ بإصدار قانون البنك المركزي والجهاز المصرفي والنقد، الجريدة الرسمية، العدد ٢٤ مكرر، ١٥ يونيه ٢٠٠٣ (السنة السادسة والأربعون).

http://www.cbe.org.eg/public/Law٪٢٠No.٨٨٪٢٠for٪٢٠٢٠٠٣.doc

- اللائحة التنفيذية للقانون رقم ٨٨ لسنة ٢٠٠٣ بقرار رئيس الجمهورية رقم ١٠١ لسنة ٢٠٠٤، منشورة بالجريدة الرسمية العدد ١٢ مكرر (أ) ٢٢ مارس ٢٠٠٤.

٢- القانون المدني المصري رقم ١٣١ لسنة ١٩٤٨.

٣- قانون التجارة رقم ١٧ لسنة ١٩٩٩.

٤- قانون التوقيع الإلكتروني رقم ١٥.لسنة ٢٠٠٤:

http://www.isdo.gov.eg/Esignature-law.asp

٥- مشروع قانون التجارة الإلكترونية المصري:

http://www.f-law.net/law/showthread.php?t=١٣٢٤٣

ب - القوانين العربية:

١- قانون المبادلات الإلكترونية التونسي رقم ٨٣ لسنة ٢٠٠٠.

http://www.arabegov.com/News/News.asp?id=٥٩١٤

٢- قانون المبادلات الإلكترونية الأردني رقم ٨٥ لسنة ٢٠٠١

www.ecipit.org.eg/Arabic/pdf/Ardon_low.pdf

٣- قانون إمارة دبي للمعاملات والتجارة الإلكترونية رقم ٢ لسنة ٢٠٠٢.

www.ecipit.org.eg/Arabic/pdf/Dubi_low.pdf

٤- قانون مملكة البحرين للمعاملات الإلكترونية ٢٠٠٢.

خامسا: المراجع باللغة الأجنبية:

- المراجع الأنجليزية:

- General Refrences:

١. **Ross Cranston,** principles of banking law, Second edition,Oxford university press, ٢٠٠٣.

٢. **Sherif Mohamed Ghanam,** Banking operations, Mansoura university- Faculty of law, (without date publishment).

- Private Refrences:

١- **A. michael Froomkin**, Article ٢B as legal software for electronic contracting- operating system or trojan horse?, Rsearch grant from the university of miami school of law, ١٩٩٨.

٢- **Adrian McCullagh and William Caelli**, Internet banking: a matter of risk and reward, springer-verlag berlin heidelberg ٢٠٠٥.

٣- **Alain Hiltgen. Thorsten kramp. Thomas**, Secure internet banking authentication, published by IEEE security&privacy, ٢٠٠٥.

٤- **AMIT YORAN**, Dveloping liability standards for electronic commerce, riptech security consulting group, USA, available at: http://www.isoc.org /inet٩٩/ proceedings/١h/١h_٢.htm

٥- **Andres Guadamuz**, Electronic money: a viable payment system?, school of law, university of Edinburgh, p ٥.avaliable at: www.era.lib.ed.ac.uk/ bitstream/١٨٤٢/٢٢٥٥/١/electronicmoney.pdf

٦- **Apostolos Ath. Gkoutzinis**, Internet banking and the law in

europe, Cambridge university press, First published, ٢٠٠٦.

٧- **Apostolos Kousaridas-George Parissis-Theodore Apostolopoulos**, An open financial services architecture based on the use of intelligent mobile devices, Electronic Commerce research and applications, ٢٠٠٧.

٨- **Benjamin Geva**, The law of electronic funds transfers, Lexis Nexis,٢٠٠١.

٩- **Brian Mantel,** Why don't consumers use electronic banking products? towards a theory of obstacles, incentives, and opportunities, Federal reserve bank of Chicago, ٢٠٠٠.

١٠- **Choi Stahl**, Electronic Payment systems, whinston, ٢٠٠٣.

١١- **Chris Reed**, Internet law, Cambridge university press, Second edition, ٢٠٠٤.

١٢- **Chris Reed**&John Angel, Computer law(the law and regulation of information tecnology), Oxford university press, sixth edition, ٢٠٠٧.

١٣- **David L. Baumer and others,** Internet privacy law: A comparison between the United States and the European Union, Computers & Security, ٢٠٠٤.

١٤- **Donald I. Baker, Roland E. Brandel**, The law of electronic fund transfer systems, alex e -solutions.inc, ٢٠٠٨.

١٥- **Gautam Ivatury, Mark Pickens**, Mobile phone banking and low-income customers, consultative group to assist the poor/the world bank and united nations foundation, ٢٠٠٦.

١٦- **Gennady Medvinsky, B.Clifford Neuman**, Net cash: a design for practical electronic currency on the internet , Information sciences institute, University of Southern California, ١٩٩٣.

١٧- **Gita Radhakrishna**, Liability issues in internet banking in Malaysia, International business information management association (IBIMA), ٢٠٠٩.

١٨- **Heather H. Bruser**, Form Contracts in an Online World: The Enforceability of Click-wrap and Browse-wrap Agreements, The Federal Lawyer, October ٢٠٠٨, p ١٤.

١٩- **James E Backhouse**, Security: the achilles heel of electronic commerce, Computer security research center - London school of economics, ١٩٩٨.

٢٠- **Jeffrey F.Rayport, bernard J.Jaworski**, Introduction to e-commerce, the mcgraw-hill companies, International

edition, ٢٠٠٣.

٢١- **Julian JB Hickey – Robin Mathew-Christopher**; E-commerce: Law, business and tax planning, Jordan's, ٢٠٠٠.

٢٢- **Katri kerem**, Internet Banking in Estonia, PRAXIS Center for Policy Studies, ٢٠٠٣.

٢٣- **Lucas D. Introna - Louise Whittaker,** Power, cash, and convenience: translations un the political site of the ATM, Taylor& francis group, LLC, ٢٠٠٦.

٢٤- **Michael chissick, Alistair Kelman**, Electronic commerce law and practice, Third edition, Saweet & Maxwell, ٢٠٠٢.

٢٥- **N.stephan Kinsella, Andrew F.Simpson,** Online contract formation, Oceana publications, First edition, ٢٠٠٤.

٢٦- **Nicholas Imparato,** Public policy and the internet, Hoover institution press,(without date publishment).

٢٧- **Nicole Atwill**, France: adapting the french legal framework to promote electronic commerce, Law library of congress, order code: LL-FLB٢٠٠٠,٠٤, June ٢٠٠٠.

٢٨- **Nikos BOGONIKOLOS**, Development of surveillance technology and risk of abuse of economic information,

European parliament, ١٩٩٩.

٢٩- **Olga Lustsik**, Can e-banking services be profitable?, Tartu university press, ٢٠٠٤.

٣٠- **Richard J. Sullivan**, How has the adoption of internet banking affected performance and risk in banks?, Federal reserve bank of Kansas city _ financial industry perspectives, ٢٠٠٠.

٣١- **Roger Leroy Miler – Gaylord A.jentz**, Law for e-commerce , West legal studies in business, ٢٠٠٢.

٣٢- **Ronald J. Mann**, Regulating internet payment intermediaries, ICEC Pittsburgh, ٢٠٠٣.

٣٣- **Satoru Torii, Yoshiki Higashikado, Takayoshi Kurita,** Framework of web applications for protection against illegal Access, FUJITSU, ٢٠٠٤.

٣٤- **Sujit Chakravorti - Victor Lubasi,** Payment instrument choice: The case of prepaid cards, Economic perspectives, Federal reserve bank of Chicago, ٢٠٠٦.

٣٥- **Thomas C. Glaessner- Tom Kellermann -Valerie McNevin**, Electronic safety and soundness, World bank working,No.٢٦, ٢٠٠٤.

٢٦- **Valters Kaze, Ilona, Erika Sumilo, Roberts Skapars**,Trends and priorities in the development of the Latvian banking services in the context of emerging knowledge based economy: case of e-banking, University of lativia, ٢٠٠٧.

٢٧- **William Gram**, Legal analysis of a banking Industry online identity and attribute authentification service for consumers and merchants: the financial service technology consortium's FAST Initiative, Federal reserve bank of Chicago, ٢٠٠٠.

٢٨- **Yoonhee Tina Chang**, Dynamics of banking technology adoption: an application to internet banking, Warwick economic research papers- university of Warwick, ٢٠٠٣.

- ***Articles:***

١- **Aaron J. Burstein**, Amending the ECPA to enable a culture of cybersecurity reseearch, Harvard journal of law & technology vol ٢٢, N ١ Fall ٢٠٠٨.

٢- ACH transactions involving the internet, Guidance and examination procedures, op. cit, P ٦. available at:

www.occ.treas.gov/ftp/bulletin/٢٠٠٤-٥٨.txt

٣- **Adel M. Aladwani**, Online banking: A field study of drivers, International journal of information management, ٢٠٠١.

٤- **Aleksander Berentsen**, Supervision and regulation of network banks, Chicago university library ,٢٠٠٧, available at: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/١٥١١

٥- **Alfred M. Pollard**, Hearing on electronic authentication and digital signature, Senate banking, housing and urban affairs committee, available at: http://www.senate.gov/~banking/٩٧_١٠hrg/١٠٢٨٩٧/witness/pollard.htm

٦- **All business**, business glossary, available at: http://www.allbusiness.com/ glossaries/virtual-banking/٤٩٤٢٠٨٨-١.html

٧- **America California Bank's Principles of Privacy**, article, available at: http://www.acbank.com/privacy.html

٨- **Andrés Guadamuz Gonzalez**, E-commerce – payment systems (PayPal: the legal status of C٢C payment systems), Computer law & security report Vol. ٢٠ no. ٤,

٢٠٠٤.

٩- **Andy Jones,** The convergence of physical and electronic security, Computer fraud& security, vol ٢٠٠٦, Issue ٣, March ٢٠٠٦.

١٠- **Anita K . Pennathur , Clicks and bricks** : E-risk management for banks in the age of the internet, Journal of internet banking and commerce (٢٠٠١).

١١- **Anna Granova& Jhp Eloff,** Online banking and identity theft: who carries the risk?, computer&farud security,(without published date).

١٢- **Authentication & Authorization for Electronic Resources,** available at: http://www.usc.edu/its/services/authx/

١٣- **Authentication in an electronic banking enviponment,** August ٢٠٠١, available at: http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

١٤- **Authentication in an internet banking environment,** Federal financial institutions examination council, available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

encyclopedia, available at: http://en. wikipedia.org/wiki/Computer_network

٢٨- **Consumer rights in electronic fund transfers**, California department of consumer affairs division of legal affairs(Legal guide CR-٦), May ٢٠٠٣.

٢٩- **Cooley Godward Llp**, Sample website development and hosting agreement, available at: http://eric_goldman.tripod. com/articles/ hostingagmt.htm

٣٠- **D McElroy and E Turban**, Smart cards in electronic commerce, International journal of information management, Vol. ١٨, No. ١.

٣١- **Dan Zhu**, Security control in inter-bank fund transfer, Journal of electronic Commerce Research, vol. ٣, no.١, ٢٠٠٢.

٣٢- **Dash, Julekha**, Who'll get the lion's share of the electronic banking, software magazine,٠٨٩٧٨٠٨٥, March ١٩٩٧, Vol. ١٧, Academic search complete.

٣٣- **Davis Jessica, Radosevich Lynda**, Safeguarding data, Vol ٢١, Issue ٨, Academic Search Complete. http://www.ebscohost.com/thisTopic.php? marketID= ١&topicID=٦٣٣

٢٤- **Denial of Service Attacks**, Coordination Center, available at: http://www.cert.org/tech_tips/denial_of_service.html

٣٥- **diretto da M.J. Bonell**, Good faith in German law and in international uniform laws, Roma ١٩٩٧, p ٩. available at: w٣.uniroma١.it/idc/centro/ publications/٢٤schlechtriem.pdf

٣٦- **Donna J. Abernathy**, Online copyrights, sep٩٩, Vol. ٥٣, issue ٩, Academic Search Premier.

٣٧- **Edward J. Obloy and B. Helen Sharetts-Sullivan**, Exploitation of intellectual property by electronic chartmakers: liability, retrenchment and a Proposal for Change, Defense mapping agency, availabl at : http://www.spatial.maine.edu/~onsrud/tempe/obloy.html

٣٨- **Edward W . Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach**, Web spoofing, technical report ٥٤٠-٩٦(revised Feb.١٩٩٧)

٣٩- **Electronic Banking Group Initiatives and White Papers**, Basel Committee for Banking Supervision, Basel October ٢٠٠٠.www.bis.org/publ/ bcbs٧٦.htm - ١٧k

٤٠- **E-statement service application form**, Terms and conditions, United overseas bank Available at :

http://www١.uob.com.mv/webpages/app_form.htm

٤١- **Everett Durante Cordy,** The legal regulation of e-commerce transactions, Journal of american academy of business, Cambridge; Mar ٢٠٠٣.

٤٢- **FCIC: electronic banking**, Electronic fund transfers, p١,avaliable at: http://www.pueblo.gsa.gov/cic_text/mony/e-banking/bank.htm

٤٣- **Ferguson, Renee Boucher**, Financial system integration tools on way, vol. ١٩, Issue ١٣, Academic Search Complete.

٤٤- **Fethi Calisir- Cigdem Altin Gumussoy**, Internet banking versus other banking channels: Young consumers' view, International Journal of information management(Science Direct), ٢٠٠٨.

٤٥- **FlexAccount**, Terms and condition, available at: http://www.nationwide.co.uk/internetbanking/help/help_FlexAccount_Terms_and_Conditions.htm

٤٦- **Fram Bureau Bank FSB**, FBB internet banking access agreement and electronic fund transfer act disclosure, available at: www.farmbureaubank.

com/docs/disclosures/IB_Agreement.pdf

٤٧- **Gabriele Lenzini, Mortaza S. Bargh and Bob Hulsebosch**, Trust- enhanced security in location-based adaptive authentication, Electronic notes in theoretical, computer science, vol ١٩٧،٢٠٠٨.

(٣)**Garcia, Erica**, What's left of the online banks, Oct ٢٠٠١, Vol . ٣٠, Issue ١٠, Academic search Premier.

(٤) **Graham Smith**, On- line banking liability, the computer law and security report, ١٩٩٦

(٥) **Hackers** , available at: http://csrc.nist.gov/publications/nistir/threats/ subsection٣_٤_٢.html

(٦) **Hanmi bank**, Hanmi internet banking service agreement, cancellation-termination of service, p. ٥. available at: http://www.hanmi.com/files/ hanmibankinternetbankingapplication.pdf

(٧) **Harry SK Tan**, Electronic transactions regulation – Singapore, Computer law & security report, Vol. ١٨ No. ٥ ٢٠٠٢.

(٨) **HiTeach**, web hosting contract, available at:

http://www.hitech-solutions. com/Contract_hosting.asp

(٩) **Holland, Bill, Billboard**, U.S.' Wipo bill is entwined with online liability issue, ٠٠٠٦٢٥١٠, ٠٩/٢٧/٩٧, Vol. ١٠٩, Billboard Journal.available at: http://www.allbusiness.com/retail-trade/miscellaneous-retail-retail-stores-not/٤٦٦١٩٢٥-١.html

(١٠) **HSBC**, Internet banking terms and conditions, available at: http://www.bahrain.hsbc.com/public/meregional/bahrain_hom/popups/en/bah_pib_terms. jhtml.

http://new.managingip.com/Article.aspx?ArticleID=١٣٢٢٠٢٠

http://projects.exeter.ac.uk/RDavies/arian/emoneyfaq.html

(١١) **IBM**, Banks form financial services net, Electronic News, Academic Search Complete, Vol. ٤٢, Issue ٢١٣٤.

(١٢) **Identity Theft and Identity Fraud,** available at: http://www.usdoj.gov/ criminal/ fraud/websites/idtheft.html

(١٣) **Identity theft**, Fighting back against, , available at: http://www.ftc.gov/bcp/edu/ microsites/idtheft/consumers/about-identity-theft.html

(١٤) **Information Security**: Guide to the electronic

communications Act. Available at: www.berr.gov.uk/files/file٩٩٨٠.pdf

(١٥) **Informix provides server for virtual bank**. (Security First National online bank will use database server from Informix), available at: http://www.highbeam.com/doc/١G١١٨٧٦٠٤٦٢.html

(١٦) **Interagency council issues guidance on electronic financial services and consumer compliance**, Federal Financial Institutions Examination Council, ١٩٩٨, http://www.ffiec.gov/pr٠٧١٥٩٨.htm

(١٧) **Internet access agreement**, First utah bank, available at: http://www. firstutahbank.com/internet_access.html

(١٨) **Internet Banking Services - Virtual Bank**, available at: http://www. clearleadinc.com/site/internet_banking.html

(١٩) **Internet Identity Theft**, Article available at: http://www.winferno.com/guides/ articles/internet-identity-theft-email-fraud.asp

(٢٠) **Internet security: distributed denial of service attacks**, OCC alert, available at: www.ffiec.gov/ffiecinfobase/resources/info_sec/occ-al_٢٠٠٠_٠١_net_sec_denial_serv_attack.pdf

(٢١) **Internet service provider**, From Wikipedia the free encyclopedia, available at: http://en.wikipedia.org/wiki/Internet_service_provider

(٢٢) **Ir.A.A.P.Schudelaro,** Electronic payment, computer law&security Report, Vol.١٧, no.٢,٢٠٠١.

(٢٣) **Is auditing guideline internet banking**, information systems audit and control association,document,G٢٤،٢٠٠٣.available at:http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=١٨٦٣٧

(٢٤) **Jim Miller,** E-money mini-FAQ, Release ٢٠٠٠.available at:

(٢٥) **John Skip Benamati - Mark A. Serva**, Trust and distrust in online banking: their role in developing countries, information technology for development, vol. ١٣ (٢) ١٦١–١٧٥, ٢٠٠٧.

(٢٦) **Jon M. PEHA,** Electronic commerce with verifiable audit trails, Carnegie mellon university USA, available at: http://www.chicagofed.org/consumer_information/what_you_should_know_about_internet_banking.cfm

(٢٧) **Jon M.peha, Ildar M. Khamitov**, paycash: A secure

efficient internet payment system, electronic commerce research and applications, Volume ٣, Issue ٤, Winter ٢٠٠٤. available at: http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B٦X٤K-٤CXMP٥B-١&_user=١٠٩٠٥٠٨&_rdoc=١&_fmt=&_orig=search&_sort=d&_docanchor=&view=c&_searchStrId=١١٧٤٣٧٥٦١٠&_rerunOrigin=google&_acct=C٠٠٠٠٥١٤٩٤&_version=١&_urlVersion=٠&_userid=١٠٩٠٥٠٨&md٥=٤cbf٠edba٦d٤e٦٧b٠٢٠٢e٦٠٣١c٥d٢١٣٦

(٢٨) **Jonathan A. Friedman- Francis M. Buono**, Limiting tort liability for online third-party content under section ٢٣٠ of the communications act, Federal communications law journal, Vol ٥٢, ٢٠٠٥.

(٢٩) **Joris Claessens- Valentin Dem- Danny De Cock-Bart Preneel- Joos Vandewalle**, On the security of today online electronic banking system, Elsevier advanced technology, Vol ٢١, No ٣.

(٣٠) **JYSKE Bank,** JBPB, net bank user agreement, (EN)-٢٠٠٧, available at: http://www.jyskebank.ch/files/netbank/JBS-NetbankUseAgreement-EN.pdf.

(٣١) **Kari Liuhto- Olga Lustsik- Mart Sorg- Janek**

Uiboupin, Organizational and sectoral changes in transition banking: Estonian experience, Journal of the Humanities&social Sciences, ٢٠٠٧.

(٣٢) **Katyal, Neal Kumar**, Crminal law in cyberspace, University of Pennsylvania law Review, Vol. ١٤٩, April ٢٠٠١,available at: http://papers.ssrn.com/sol٣/papers.cfm?abstract_id=٢٤٩٠٣٠&rec=١&srcabs=٥٩٤١٠١

(٣٣) **Kevin J.Houle, George M. Weaver**, Trends in denial of service attack technology, Coordination center,Vo١,٠,October ٢٠٠١.

(٣٤) **Kit Burden**, Electronic commerce proposals-UK, Computer law & security report Vol. ١٥, N ٤, ١٩٩٩.

(٣٥) **Laura Darden , Charles Thorpe,** Forming contracts over the internet: click-wrap and browse-wrap agreements, Georgia state University, Law and the internet Journal - Summer ٢٠٠٣.

(٣٦) **Legal protection**, Computer programs, available at: http://europa.eu/ scadplus/leg/en/ lvb/l٢٦٠٢٧.htm

(٣٧) **Lorna Gillies**, Jurisdiction for consumer contracts,

Computer law & security report, vol. ١٧ No. ٦, ٢٠٠١.

(٣٨) **M.Sklira. A.S.pomportsis. M.S. Obaidat.** A framework for the design of bank communications, computer communication, ٢٠٠٣. available at: www.ComputerScienceWeb.com

(٣٩) **Manfred mueller**, Smart card readers bring security online in Germany, January ٢٠٠٤, available at: www.contactless-club.com Bank of Internet USA, Privacy Policy, January ٢٠٠٦, available at: http://www.bankofinternet.com/ privacy-policy.aspx

(٤٠) **Marie Wright,** Authenticating electronic cash transactions, Computer fraud & security, April ١٩٩٧.

(٤١) **Mark Owen, Richard Penfold**, Copyright infringement in the on-line world, The global magazine for Intellectual property owners, Dec٩٩/ Jan ٢٠٠٠, Issue ٩٥, available at:

(٤٢) **Mark Turner and Mary Traynor, Herbert Smith**, UK e-commerce liability, Computer law & security report, Vol. ١٩, no. ٢, ٢٠٠٣.

(٤٣) **Martin Sloan,** Web accessibility and the DDA, Journal of Information, Law and Technology, ٢٠٠١.

(٤٤) **MCB internet banking**, available at: http://www.mcb.mu/documents/terms/ ibterms.html

(٤٥) **Michael D. Scott**, Liability in cyberspace – III, Computer law & security report, vol. ١٣, no. ٦, ١٩٩٧.

(٤٦) **Michael P. Dierks**, Computer network abuse, Harvard Journal of law, Vol ٦, Spring Issue, ١٩٩٣.

(٤٧) **Michael S. Baum and Henry H. Perritt**, Electronic contracting publishing, and ED١ law. Government information Quarterly, Vol. ١, No. ١. ١٩٩١.

(٤٨) **Money laundering**: a banker's guide to avoiding problems, (OCC), second edition, ٢٠٠٢.

(٤٩) **Mukesh M. Prabhu, S.V. Raghavan**, Security in computer networks and distributed systems, Computer communications, ١٩٩٦(٣٧٩-٣٨٨).

(٥٠) **Neil Chou and others**, Client-side defense against web-based identity theft, Stanford University, Stanford CA ٩٤٣٠٥, (without publishment date).

(٥١) **Net Bank**, Open an account, available at: https://Secure.netbank.com/cgi-bin/universe?LM=٥٦

(٥٢) **Net Cash Terms of Use**, Your

Representations/Warranties, available at: https://www.netcash.com/engine/show?topic=terms

(٥٣) **NetBank**, how NetBank help to protect you, Available at: http://www. netbank.com/about_security_how_protect.htm

(٥٤) **Nigel Miller**, UK E-commerce bill - progress?, Computer fraud & security, november ١٩٩٩.

(٥٥) **Oliver Lau,** meta-firewall: a sixth generation firewall, elsevier science Ltd, ١٩٩٨.

(٥٦) **Online banks heat up competition with savings rates of ٥٪ or more**, Academic Search Premier, FEB ١٣. ٢٠٠٧.available at: http://www.bankrate.com/

(٥٧) **Online Liability decision stands**, Editor& Publisher, ٠٠١٣٠٩٤X, ١/١٣/٩٦, Vol. ١٢٩.

(٥٨) **Paola Garrone- Massimo G. Colombo**, market-driven design of innovative services The case of multimedia home banking, elsevier Science Ltd, ١٩٩٩.

(٥٩) **password cracking**, available at : http://www.webopedia.com/TERM/ P/password_cracking.html

(٦٠) **Password**, From Wikipedia, the free encyclopedia, available at: http://en. wikipedia.org/wiki/Password

(٦١) **PayCash**, Term s &Conditions, Right/responsibilities of cyphermint users, http://www.paycashwallet.com/consumer/TermsAndConditions.html

(٦٢) **Peer-to-peer**, From Wikipedia, The free encyclopedia, available at; http://en.wikipedia. org/wiki/Peer-to-peer

(٦٣) **peter spencer**,Regulation of the payments market and the prospect for digital money, BIS papers, No ٧.

(٦٤) **Principles for electronic authentication**, the authentication principles working group, e-commerce branch industry canada. www.ic.gc.ca/eic/ site/ecic-ceac.nsf/vwapj/Authentication.pdf/$file/Authentication.pdf

(٦٥) **Privacy**, From Wikipedia, the free encyclopedia, available at http://en. wikipedia.org/wiki/Privacy

(٦٦) **Reducing the risk of identity theft**, available at: http://www. privacyrights.org/fs/fs١٧-it.htm

(٦٧) **Richard H. Paine**, Secure mobile architecture (SMA– A way to fix the broken Internet), Information on security technical report, Vol ١٢, Issue ٢, ٢٠٠٧.

(٦٨) **Richard J. Sullivan**, Risk management and nonbank participation in the U.S. retail payments system, Federal

reserve bank of Kansas City, P٦. available at: www.KansasCityFed.org

(٦٩) **Risk management principles for electronic banking**, Basel committee Publication, July ٢٠٠٣, Available at: http://www.bis.org/pub١/bcbs٩٨.htm

(٧٠) **Rob Rachwald**, Is banking online safer than banking on the corner? Computer fraud & security, ٢٠٠٨.

(٧١) **Roger Dean and others**, Identity management – back to the user, Network security, December ٢٠٠٦.

(٧٢) **Roger Dean**, Identity management back to the user, Network security puplishment, December ٢٠٠٦.

(٧٣) **Rosa Julia-Barcel٥ -Thomas C. Vinje**, Electronic signatures, Computer law & security report Vol. ١٤ no. ٥ ١٩٩٨.

(٧٤) **Rosa Julia-Barceld**, Electronic contracts, computer law & security report vol. ١٥, No. ٣ ١٩٩٩.

(٧٥) **S.K. Leong T. Srikanthan, G.S.Hura**, an internet application for on-line banking, Computer Communication, Elsevier, ١٩٩٧.

(٧٦) **Sangjun Lee-SeungBae Park**, Mobile password system

for enhancing usability -guaranteed security in mobile phone banking, Springer- verlag berlin heidelberg, ٢٠٠٥.

(٧٧) **Scott F. Uhler, Philippe R. Weiss , Michele M. McGee,** Liability issues and the internet Part ١: electronic mail, available at : http://www.lib.niu.edu/ipo/١٩٩٦/il٩٦. ٢٦٦.html

(٧٨) **Shaoyi Liaoa and other**, The adoption of virtua banking: an empirical study, international journal of information management, ١٩٩٩.

(٧٩) **Shirley Radack,** Electronic authentication: guidance for selecting secure techniques, available at: http://www.itl.nist.gov/lab/bulletns/bltnaug ٠٤.htm

(٨٠) **Simon Newman, Gavin Sutter**, electronic payments-the smart card, Computer Law& Security Report Vol. ١٨ no. ٥ ٢٠٠٢.

(٨١) **Sofia Giannakoudi**, Internet banking: the digital voyage of banking and money in cyberspace, Information & Communications Technology Law, vol.٨, No.٣, ١٩٩٩.

(٨٢) **Stan J. Liebowitz&Stephen Margolis**, Seventeen famous economists weigh in on copyright: the role of

theory, empirics, and network effects, Harvard journal of law & Technology, Vol ١٨, No ٢, Spring ٢٠٠٥.

(٨٣) **Steelcity web services**, web site design agreement, available at: http:// www.steelcitywebservices.com/downloads/webagreement.pdf

(٨٤) **Steffen Lippert, Giancarlo Spagnolo,** Internet peering as network of relations, telecommunications policy, February ٢٠٠٨, Vol ٣٢, Issue ١

(٨٥) **Stephen Rawson, Partner, Denton Wilde Sapte,** E-commerce- mobile transactions,computer law & security report, Vol.١٨, no.٣, ٢٠٠٢.

(٨٦) **Susannah Fox and Jean Beier**, Online banking ٢٠٠٦: Internet & American Life Project, June ١٤, ٢٠٠٦.

(٨٧) **Tahir Masood Qureshi,** Customer acceptance of online banking in developing economies, Journal of internet banking and commerce, April ٢٠٠٨, vol.١٣, no.١, available at: http://www.arraydev.com/commerce/jibc/

(٨٨) **Tanai Khiaonarong**, Electronic payment systems development in Thailand, International journal of information management,٢٠٠٠.

(٨٩) **The Internet and the USA Patriot act**: Potential implications for electronic privacy Security Commerce and Government, CRS Report for Congress, Order Code RL٣١٢٨٩. availabl at: epic.org/privacy/terrorism/usapatriot/RL٣١٢٨٩.pdf

(٩٠) **The new banking delivery system-the internet, goodwin,** Procter& Hoar LLp, vol.٢ No.٣٥, April ٢٧, ١٩٩٩.

(٩١) **Thierry Moreau**, The emergence of a legal framework for electronic transactions, Computers & security, Vol ١٨،١٩٩٩.

(٩٢) **Thierry Moreau**, The emergence of a legal framework for electronic transactions, computers & Security, ١٩٩٩.

(٩٣) **Threat Identification Resource**, CMS Information Systems, Center for Medicare& Medicaid Services, Version ١,٠, May ٧, ٢٠٠٢, p ٧ available at : http://csrc.nist.gov/fasp/FASPDocs/risk-mgmt/Threat_ID_resource.pdf

(٩٤) **Tom Arnold,** Internet identity theft, Technology working group, E -business division. June ٢٠٠٠.

(٩٥) **Transactional Banking Services Conformed Contract**, SA Govt Transaction Banking Contract,

November ٢٠٠٢.available at:

(٩٦) **Turner Shawn,** U.S. anti-money laundering regulation: an economic approach to cyberlaundering, Case western reserve university school of law, vol ٥٤:٤, ٢٠٠٤.

(٩٧) **U.S. consumers and electronic banking,** ١٩٩٥-٢٠٠٣, available at: www.federalreserve.gov/pubs/ bulletin/٢..٤/winter.٤_ca.pdf

(٩٨) **Validation test begins for Japan's first electronic authentication system,** available at: http://www.nmda.or.jp/nmda/commerce/kousyou-english.html

(٩٩) **Website design agreement,** House media, available at: http://www.ihm. co.uk/terms/Design-Terms.pdf

(١٠٠) **Website design process,**Vivid internet production, available at: http://www. biztree.com/Templates/Website-Design-Agreement.html

(١٠١) **Website hosting contract and terms of services agreement,** available at: https://secure٧.hostek.net/contract.shtml

(١٠٢) **Website Spoofing,** available at :http://strategis.ic.gc.ca/epic/site/cybpr-cybi. nsf/en/h_wd٠٠١٦٢e.html

(١٠٣) **Working group on international consensus principles for electronic authentication**, internet law& policy forum, ٢٠٠٥.availabl at: http://www. ilpf.org/events/intlprin.htm

www.treasury.sa.gov.au/public/download.jsp?id=٢٤٨١

(١٠٤) **Yao-Hua Tan - Walter Thoen**, INCAS: A legal expert system for contract terms in electronic commerce, Elsevier cience B.V, (Decision Support Systems), ٢٠٠٠. www.elsevier.comrlocaterdsw

(١٠٥) **Yoonhee Tina Chang**, Dynamics of internet banking adoption, ESRC centre for competition policy- University of East anglia, ISSN ١٧٤٥-٩٦٤٨, October ٢٠٠٥.

(١٠٦) **Yougu Yuan and others**, Web spoofing ٢٠٠١, available at : www.cs. dartmouth.edu/pkilab/demos/spoofing/

- ***Thesis:***

- **Charles A. Oswald,** legal and policy analysis of informal and formal money Transfer systems, (a comparative historical), dissertation presented to school of law, saint Thomas university, December ٢٠٠٧.

- **G C CHALIKIAS**, A guideline concerning electronic banking services- the case of greece, MSc thesis to school of industrial and manufacturing science-cranfiled university, Academic year ٢٠٠٣ –٢٠٠٤.
- **Haibo Huang**, Essays in electronic money and banking, dissertation- faculty of the graduate school, university of Taxes, ٢٠٠٥.
- **Jaakko Vilén**, Accessibility in internet services – case electronic banking, Master's Thesis, HesnkiI versity of technology, available at: lib.tkk.fi/Dipl/ ٢٠٠٦/urn٠٠٧٥٢٥.pdf
- **Jeanette Taft**, An examination of the antecedents of electronic banking technology acceptance and use, Dissertation, college of business administration –Touro university international, ٢٠٠٧.
- **Jennifer Iser**, Across country analysis of the effects of E-banking and financial infrastructure on financial sector competition, dissertation, school of business-Nova southeaster university, ٢٠٠٨.
- **Meiring, Gezina Aletta** , Legal aspects of the computerisation of the payment system, Dissertation

presented to University of South Africa (South Africa), DAI-A ٦١/٠٣, Sep ٢٠٠٠.

- **Pormita shaha yanni zhao**, Relationship between online service quality and customer satisfaction (a study in internet banking), Master thesis, department of businees administration and social sciences- lulea university, ٢٠٠٥, p ٣

- **Rexnold Elias Byers**, Structuring service delivery processes: an examination of problems in retail banking and telephone center design, dissertation, school of business Administration, university of Rochester, ٢٠٠٠.

- **Zakaria I.Saleh**, An examination of the internet security and its impact on trust and adoption of online banking, dissertation, Capella, ٢٠٠٣.

- Journals:

- Electronic Journal of Law.
- Federal communications law journal.
- Harvard Journal of Law.
- Information & Communications Technology Law .

- International Journal of Information Management, .
- Journal of American Academy of Business, Cambridge.
- Journal Of Banking & Finance.
- Journal of Electronic Commerce Research.
- Journal of International Accounting, Auditing & Taxation.
- journal of Internet Banking and commerce.
- Journal of the Humanities & social sciences.
- journal on the internet.
- Texas international law journal.

- *Conferences:*

- **Avery W. Katz,** Is electronic contracting different? contract law in the information age, travemünde conference on the economic analysis of law, ٢٠٠٤. www.columbia.edu/~ak٤٧٢/papers/Electronic٪٢٠Contracting.pdf
- **John Carlson, Karen Furst, William W.Lang, Daniel E.Nolle**, Internet banking: market developments and regulatory issues, society of government economists conference, May٢٠٠١. www.occ.treas.gov/netbank/

SGEC٢٠٠٠.pdf

- **Uniform computer information transaction ACT**, on uniform state laws, annual conference, Colorado, July ٢٣-٣٠, ١٩٩٩. www.law.upenn.edu/bll/archives/ulc/ucita/٢٠٠٢final.pdf

Judgments:

- United States Court of Appeals , Judgment of the Court of Justice in Case C-٢٧٥/٠٦, PRESS RELEASE No ٥/٠٨,.
- United States Court of Appeals, autumn ٢٠٠٦, (Plant *v* Service Direct), available at.
- United States Court of Appeals for the Federal Circuit, BMC Resources.Inc. V.Paymentech, L.P ٢٠٠٦-١٥٠٣.
- United States Court of Appeals for the Federal Circuit, Decisioning, INC., ٢٠٠٧-١٢٧٧.
- United States Court Of Appeals For The Ninth Circuit, (Kremen v Cohen), ٣٣٧ F.٣d ١٠٢٤; ٢٠٠٣ U.S. App. LEXIS ١٤٨٣٠; ٦٧, No. ٠١-١٥٨٩٩, July ٢٥, ٢٠٠٣.

- Reports

- **Apec electronic commerce task force**, Background Report

on Electronic Commerce , ١٩٩٨.

- **Basel Committee On Banking Supervision**, Management and Supervision of Cross- Border Electronic Banking Activities, July ٢٠٠٣.

- **Central Bank of Malta**, electronic payment services, Report No ٤, January ٢٠٠٨.

- **Comptroller of the Currency** , Decision of the Office of the Comptroller of the Currency on the application to charter, Conditional Approval (٣٤٧), January ٢٠٠٠.

- **Comptroller of the Currency Administrator of National Banks** , Internet Banking, Comptroller Handbook, , October ١٩٩٩.

- **Comptroller of the Currency Administrator of National Banks** ,Threat from Fraudulent Bank Web Sites, July ١،٢٠٠٥.

- **Comptroller of the Currency, Administrator of National Banks,** Corporate Decision# ٩٩-٥٠, January ٢٠٠٠.

- **Comptroller of the Currency, Internet access service,** Interpretive Letter No (٧٤٢), August ١٩, ١٩٩٦.

- **CRS Report for Congress**, The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government.
- **European central bank**, Report on electronic money , augest ١٩٩٨.
- **Federal Deposit Insurance Corporation** ,Tips for Safe Banking Over the Internet, September ٢٠٠٠.
- **Federal Financial Institutions Examination Council**, E-Banking, IT examination handbook, august ٢٠٠٣.
- **Federal Reserve Bank of Dallas**, Request for Public Comment on a Proposal to Revise the Official Staff Commentary to Regulation E (Electronic Fund Transfers) , Vol. ٦٥, No. ١٢٦, July ٢٠, ٢٠٠٠.
- **The Federal Reserve Board**, Electronic Fund Transfers, Consumer Handbook to Credit protection Laws, August ٢٠٠٧.

- Laws

- (Financial Modernization Act) http://banking.senate.gov/conf/summ.pdf
- (OPPA)

http://www.kronishlieb.com/files/tbl_s٢٤News٪٥CPDFUpload١٥٢٪٥C٩٢٧٪٥CALERT -Cal_OPPA.pdf

- Chinese Internet Regulations on the Administration of Internet publishing ٢٠٠٠.
- Digital Signature and Electronic Authentication Law (SEAL) of ١٩٩٨ (Introduced in Senate), available at; http://thomas.loc.gov/cgi-bin/query/z? c١٠٥:S.١٥٩٤.IS
- Electronic Communications Privacy ACT of ١٩٨٦, available at: http://www. cpsr.org/issues/privacy/ecpa٨٦
- Electronic Transactions ACT ١٩٩٨, Legal Guide to the Electronic Transactions ACT, available at: www.ida.gov.sg/doc/Policies٪٢٠and٪٢٠ Regulation/Policies_and_Regulation_Level٣/Legal_Guide_١٩٩٨.pdf
- Monetary and financial code; http://١٩٥,٨٣,١٧٧,٩/upl/pdf/code_٢٥.pd
- Spain's Electronic Signatures Act www.ibls.com/members/docview.aspx? doc=١٨١٧ - ٢٧k
- UK Electronic Communications Act ٢٠٠٠. www.opsi.gov.uk/Acts/acts٢٠٠٠/ pdf/ukpga_٢٠٠٠٠٠٠٧_en.pdf
- UNCITRAL Model Law on Electronic Commerce ١٩٩٦.

www.uncitral.org/ pdf/english/texts/electcom/٠٥-٨٩٤٥٠_Ebook.pdf

- UNCITRAL Model Law on Electronic Signatures ٢٠٠١. www.uncitral.org/pdf/ english/texts/electcom/ml-elecsig-e.pdf.
- Uniform Commercial Code, ١٩٩٧,. http://www.law.cornell.edu/ucc/ucc. table.html

Directives:

- Directive ,٢٠٠٢/٥٨/EC. Official Journal of the European Communities, ١٢ July ٢٠٠٢.
- Directive ١٩٩٩/٩٣/EC , Official Journal of the European Communities, December ١٩٩٩.
- Directive ٢٠٠٠/٣١/EC . Official Journal of the European Communities, June ٢٠٠٠.
- Directive ٢٠٠٠/٤٦/EC , Article (١), Official Journal of the European Communities, ١٨ September ٢٠٠٠.
- Directive ٢٠٠٢/ EC,(Privacy and Electronic Communications), Official Journal of the European Communities, ٢٠٠٢.

* Directive ٢٠٠٢/٥٨/EC, (Directive on privacy and electronic communications), ٢٠٠٢
* Directive ٩٣/١٣/EC, on unfair terms in consumer contracts, Official Journal of the European Communities,٥ April ١٩٩٣.
* Directive ٩٧/٧/EC, (on the protection of consumers in respect of distance contracts), Official Journal of the European Communities, ٢٠ May ١٩٩٧.

- ***Electronic Site:***

٥- موقع مكتب تسجيل حقوق الملكية الفكرية الأمريكي .

http://www.copyright.gov/

٦- موقع مكتب الاحتياطي الفيدرالي الأمريكي

http://www.federalreserve.gov/

٧- موقع مكتب الرقابة على النقد الأمريكي

http://www.occ.treas.gov/

٨- موقع المنظمة الدولية لهيئات الأوراق المالية

http://www.iosco.org/

٩- موقع لجنة نظم الدفع والتسوية

http://www.bis.org/cpss/index.htm

١٠- موقع لجنة القانون التجاري التابع لمنظمة الأمم المتحدة

http://www.uncitral.org/

١١- موقع غرفة المقاصة ونظم التسوية بين البنوك

http://www.chips.org/home.php

١٢- موقع الجمعية المالية للاتصالات السلكية واللاسلكية بين البنوك

http://www.swift.com/

١٣- موقع الجمعية الوطنية لنظم التسوية الآلية

http://www.nacha.org/

١٤- موقع الأمانة العامة لتكنولوجيا الصناعة المصرفية

http://www.bitsinfo.org/

١٥- موقع لجنة التجارة الاتحادية .

http://www.ftc.gov

١٦- موقع البنك المركزي الأوربي

http://europa.eu/institutions/financial/ecb/index_en.htm

١٧- موقع البرلمان الأوربي

http://www.europarl.europa.eu/news/public/default_en.htm

سادسا- المراجع الفرنسية:

-Livers:

-**Carlos Martin& Denis Beau**, les services financiers en ligne, Rapport du groupe de travail, présenté au comité d'orientation, N ٥, ١٥ novembre ٢٠٠١,provident du site:

http://www.telecom.gouv.fr/fonds_documentaire/men/ecotic//rapport٥.pdf

-**Francois Dentz**, la banque et l'utilisation de swift, Transplis, No special, avril ١٩٧٥.

-**Francilon,** Infractions relevant du droit de l'information et de la communication, Rev. sc. crim, juill. ١٩٩٩

-**Jacques vanrenterghem**, Un projet international de commutations de messages interbancaires, Organisation et technique bancaires, N ٣٢٨-avril ١٩٧٤.

-**Jean Pionnier**, Sécurité informatique (un nouvea souci de l'inspection bancaire), Theme de la Journée organisée le mercredi , No٣-Mars ١٩٨٥.

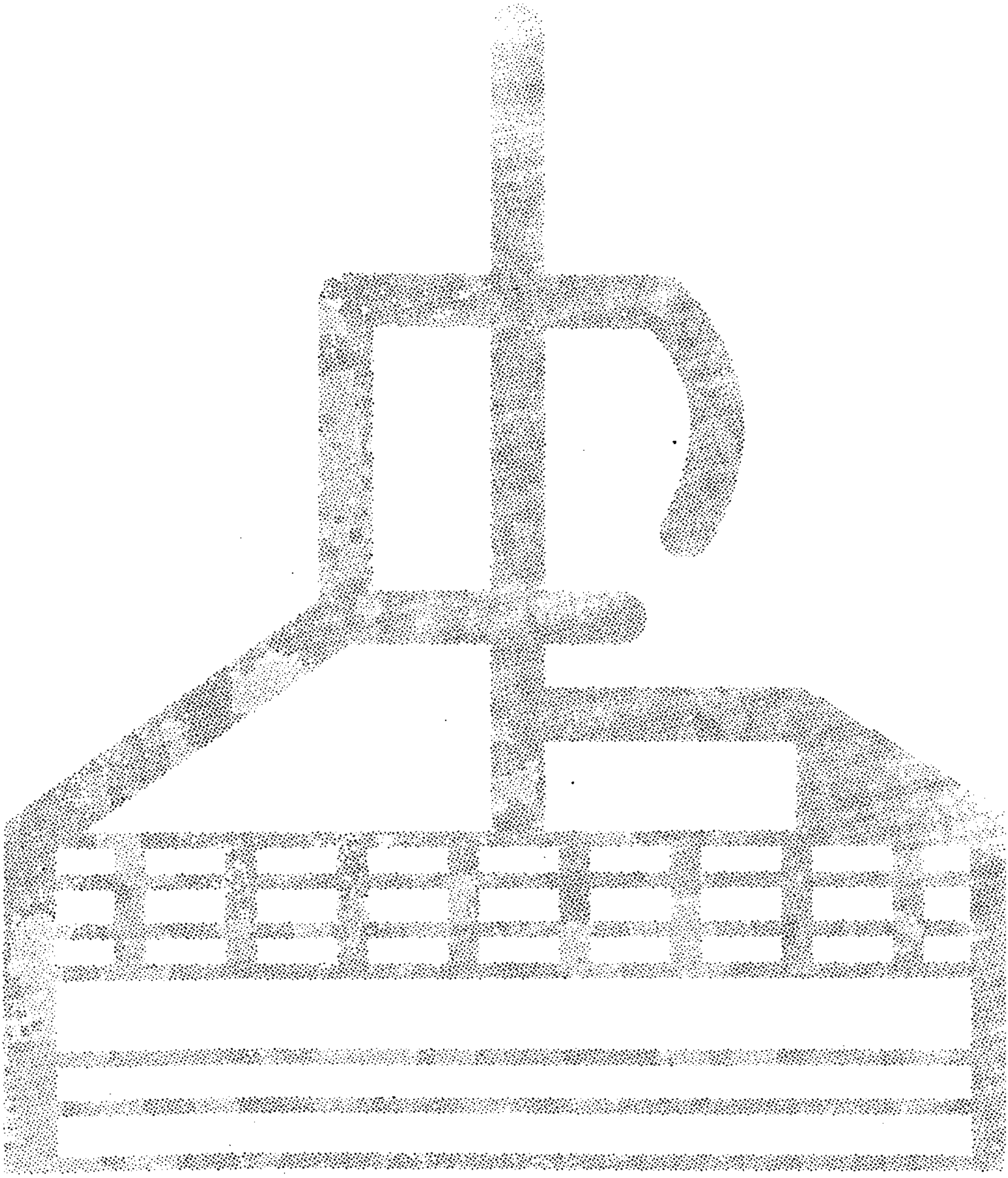
-**Julien le Clainche**, L`adaptation des droits du paiement français et américain aux nouvelles technologies, p ١٥, provident du site: www.droit-ntic.com

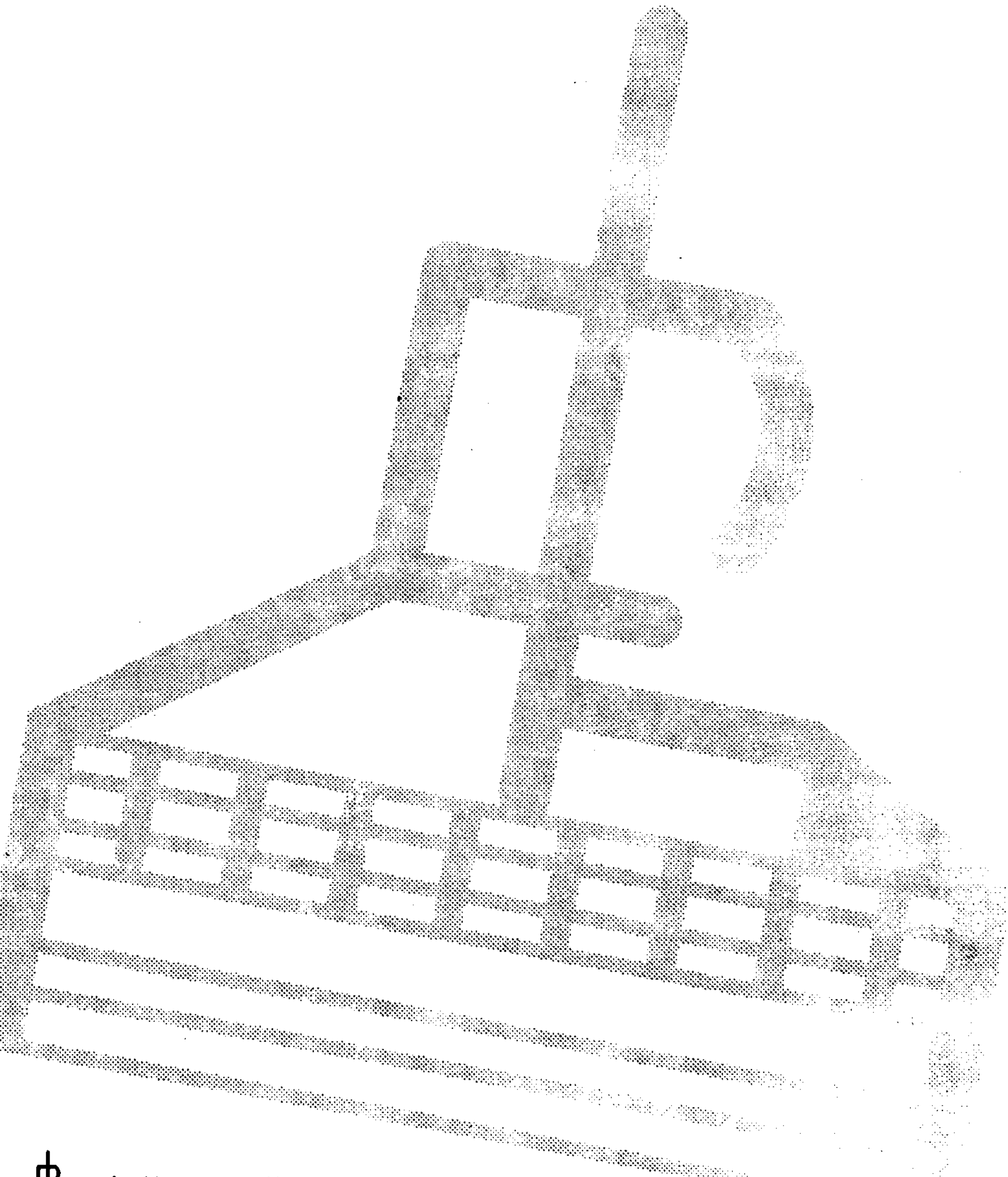
- *Jugements:*

- C A Pairs.٥e ch ٤ Janv, ١٩٨١.
- C A Pairs ٥e ch, ٦ mars ١٩٨١.
- CA Paris. ١٤ janv. ١٩٩٧, Juris-, n° ٢٠١٢٨.
- CA Paris. Juris-Data, n ٠٢٠١٢٨, ١٤ janv.١٩٩٧.
- Paris, ٥ avr. ١٩٩٤, D. ١٩٩٤, Flash, n ١٨.
- Paris, Flash, n° ١٨, ٥avr. ١٩٩٤.
- Crim, ٢/٤/١٩٧٤, crim, n ١٣٩, ١٩٧٤,
- Crim, ٤/١/١٩٦٨, Bull. crim, n ١, Rec. D, ١٩٦٨.

قائمة المحتويات

رقم الإيداع	٢٠١١/١٥٥٢
الترقيم الدولى	I.S.B.N
978-977-328-824-0	





دار الجامعة الجديدة للنشر

٣٨ شارع سوتير - الأزاريطة الإسكندرية ت : ٤٨٦٣٦٢٩ - ٤٨٦٨٠٩٩

E-mail. : darelgamaaelgadida@hotmail.com

www.darggalex.com info@darggalex.com

دار الجامعة الجديدة

٣٨ - ٤٠ ش سوتير - الأزاريطة - الإسكندرية
تليفون : ٤٨٦٣٦٢٩ فاكس : ٤٨٥١١٤٣ تليفاكس : ٤٨٦٨٠٩٩
E-mail : darelgamaaelgadida@hotmail.com
www.darggalex.com info @ darggalex.com